Privacy, Security and Other Personal Issue in e - Commerce

Payal M. Chitrani
Faculty,
Swami Sahajanand College of Commerce & Management,
Bhavnagar.

Received Feb 20, 2015 Accepted March 10, 2016

ABSTRACT Without trust, most prudent business operators and clients may decide to forgo use of the Internet and revert back to traditional methods of doing business. To counter this trend, the issues of network security at the ecommerce and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended e-commerce operation. This paper will discuss present some of the threats to e-commerce and customer privacy also legal aspects and other non-technical issues of E-commerce. With the rapid expansion and use of E-commerce, privacy has become an ongoing and increasing concern for the users, providers, technologist as well as the policy makers. While it is difficult to complete a transaction in e-commerce by a user without providing private information, protecting that information from proliferating is another difficult issue for the providers, technologist and the policy makers. Psychologically, users' of e-commerce are unwilling to provide private information or even to browse online if they believe their privacy is not protected. Fortunately, there are technologies as well as policies are in effect, as well as are in development stages to help protect privacy at current and in future. However, there is a need to know more about the range of privacy issues in order to build usable and effective mechanisms for those companies and other privacy protection technologies and policies. This paper presents previous, existing and future privacy issues and their solutions in respect of e-commerce also in this paper, the reasons behind lack of customer security and privacy online are discussed; importance of adequate security and privacy measures is emphasized, and a few methods to implement the change are outlined. This article is based on a literature review that emphasizes the need for increased security and privacy measures and the importance of customers trust in developing online relations.

Key words: privacy, security and personal issue.

INTRODUCTION

By Internet commerce, we mean the use of the global Internet for purchase and sale of goods, services, including service and support after sale. E-Commerce means buying and selling goods and products over internet.

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. In e-commerce development security is a critical factor to consider. It is one of the pivotal success factors of e-commerce. Security is defined as “the protection of data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction”. It usually refers to the provision of access control, privacy, confidentiality, integrity, authentication, non-repudiation, availability and effectiveness. Surveys conducted and compiled recently shows increasing concerns on security risks and have become a global issue. When customers lose confidence in a systems ability to protect sensitive and confidential data such as credit card information its feasibility will be compromised. The system t thus will be rendered helpless.

Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for e- Commerce providers. Personal information has always been technically available but its access to the public was limited, the tremendous growth of the internet however simplified the process and now private information can be viewed with a simple mouse click. Consumer privacy is replacing theft and fraud as top customer concerns for e-commerce. It was discovered from a study based on tracking and history recording technologies that users showed great concern in terms of privacy on the above mentioned technologies. It is therefore clear the adverse effects that lack of privacy or privacy concerns have on e-commerce success. Companies are advised to tailor solutions to these problems in order to achieve higher market penetration.

The exponential growth of the Internet and online activity raise a number of new regulatory issues and legal questions. How does copyright apply to digital content? How can national laws apply to activities in cyberspace? Can privacy and data protection exist on the Web? Can electronic commerce really be secure? Should governments tax cyber trade? Can cyberspace be regulated by one, or by many authorities? In seeking to apply the law to the Internet, problems arise owing to the fact that most laws largely apply to the pre-cyberspace world. In the modern era of electronic technology, many people want to get their work done quickly with little effort. At times, people forget or do not consider the legal and ethical values of their procedures. In traditional commerce, it's not easy to start a business. You must implement strategies that follow rules and regulations enforced by government. Electronic commerce makes it possible to do almost any kind of business in a very simple way. What makes it simple? The reason is that existing legal frameworks and enforcement mechanisms are not strong.E-commerce presents a world of opportunity for doing businesses, reaching global markets and purchasing without leaving the home or office. E-commerce can provide opportunities to improve business processes, just as phones, faxes and mobile communications have in the past. However, just as any new business tool has associated issues and risks so does e-commerce. It’s important to understand the legal issues and potential risks to ensure a safe, secure environment for trading with customers and other businesses. The issue of law on the Internet is a complex one. Between the two all-or-nothing extremes lies a broad spectrum of possibilities. Many people revel in the freedom to express themselves and the freedom from prohibitions such as zoning restrictions that the Internet apparently affords. With no law at all, however, the Internet would be no place to conduct business or pleasure. Laws give people certainties about their rights and responsibilities: they make life more predictable.

The Threats to E-Commerce

Three types of security threats

–denial of service,

–unauthorized access, and

–theft and fraud

I. Security (DOS): Denial of Service (DOS)

•Two primary types of DOS attacks: spamming and viruses

•Spamming

–Sending unsolicited commercial emails to individuals

–E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.

–Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.

–DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target

•Viruses: self-replicating computer programs designed to perform unwanted events.

•Worms: special viruses that spread using direct Internet connections.

•Trojan Horses: disguised as legitimate software and trick users into running the program.

II. Security (unauthorized access)

•Illegal access to systems, applications or data

•Passive unauthorized access –listening to communications channel for finding secrets.

–May use content for damaging purposes

•Active unauthorized access

–Modifying system or data

–Message stream modification

•Changes intent of messages, e.g., to abort or delay a negotiation on a contract

•Masquerading or spoofing –sending a message that appears to be from someone else.

•Sniffers–software that illegally access data traversing across the network.

•Software and operating systems ‘security holes.

III. Security (theft and fraud)

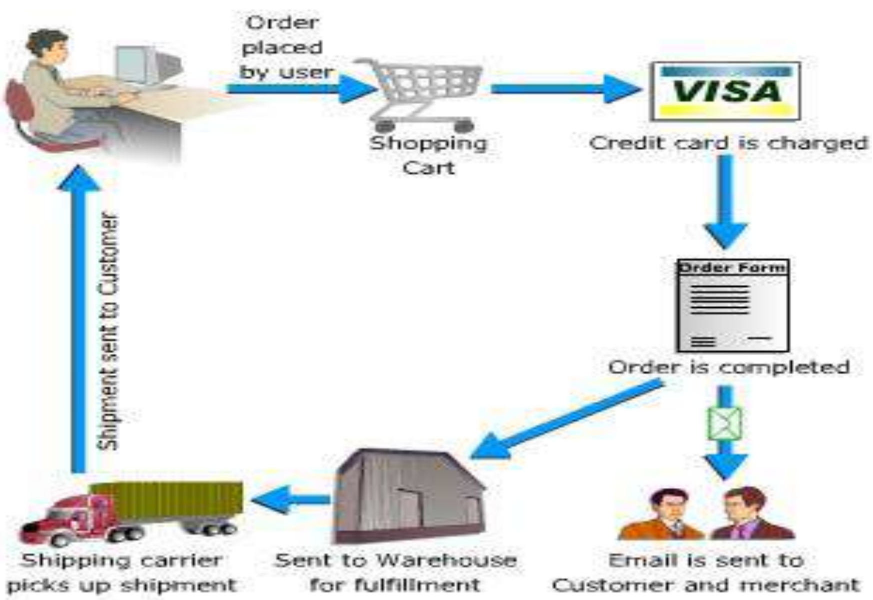
•Data theft already discussed under the unauthorized access section

•Fraud occurs when the stolen data is used or modified.

•Theft of software via illegal copying from company‘s servers.

•Theft of hardware, specifically laptops.

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. A transaction between buyers and sellers in e-commerce includes requests for information, quotation of prices, placement of orders and payment, and after sales services. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet. Privacy and security can be viewed as ethical questions. At the same time the privacy and security area attracts a large amount of attention from the commercial sector because it has the potential to determine the success or failure of many business ventures, most obviously ecommerce activities.


Order placed by user
Shopping Cart
VISA
Credit card is charged
Order Form
Order is completed
Email is sent to Customer and merchant
Sent to Warehouse for fulfillment
Shipping carrier picks up shipment
Shipment sent to Customer

PURPOSE OF SECURITY,

1. Data Confidentiality – is provided by encryption /decryption.

2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.

3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.

4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.

Technical Components of eCommerce Security

There are four components involved in ECommerce Security: client software, server software, the server operating system, and the network transport. Each component has its own set of issues and challenges associated with securing them:

- Client software is becoming increasingly more security-focused, however single-user desktop operating systems historically have had no security features implemented. ECommerce software that relies on the security of the desktop operating system is easily compromised without the enforcement of strict physical controls.
- Server software is constantly under test and attack by the user community. Although there have been cases of insecurities, a system administrator keeping up with the latest patches and vendor information can provide a high degree of confidence in the security of the server itself.
- Operating systems used for hosting Ecommerce servers are securable, but rarely shipped from the vendor in a default configuration that are secure. Ecommerce servers must protect the database of customer information accumulating on the server as well as provide security while the server is handling a transaction. If it is easier for a thief to compromise the server to obtain credit card numbers, why bother sniffing

the network for individual credit card numbers?

- Session transport between the client and server uses network protocols that may have little or no built-in security. In addition, networking protocols such as TCP/IP were not designed to have confidentiality or authentication capabilities.

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have following categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought specific merchandise.
- Integrity: prevention against unauthorized data modification
- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
- Availability: prevention against data delays or removal.

Possible Enhancements:-

It is however possible to improve and enhance current security measures in ways that ensure higher customers satisfaction and trust. In most organization, security is an afterthought rather than an integral part of the infrastructure and companies are usually cost driven rather than value driven when it comes to security. This should change and E-commerce sites should find ways to improve and tailor their security according to customer needs and demands. Software developers must develop software to enhance safety and security and provide safety measures like encryption, digital signatures, biometrics, virus protection, etc. Introducing security seals is also advisable. Moreover, educating customers on security issues and how to protect their computers is also a major part of the security implementation process. Therefore, as can be seen, in order for e-commerce security to blossom, it is important to look at it from 24 many different angles, and focus on not only the company's guarantees, but also on customer's needs and the initial software development process. Security must also be achieved in a collective manner rather than individualistic in order to improve the worldwide perception of online security.

PRIVACY ISSUES:-

The word "Privacy" could be described as the right to be left alone, or the right to exercise control over one's personal information, or a set of conditions necessary to protect dignity and autonomy of an individual.

E-COMMERCE FRAMEWORK AND PRIVACY ISSUES

Trading in the online shop accessed through internet between business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) is the main purpose of e-commerce. Parties involved in this kind of trading exchange information including private information like addresses (exchanged as mailing/billing information), credit card number (exchanged for payments), etc. to complete a transaction. Here is the catch; information exchanged by the parties is stored and warehoused for other business purposes like direct marketing, research, selling to third parties, etc.

E-commerce is considered as a powerful tool to collect consumer's private information. The same tool and their use in business also interfere on the privacy of individuals. Monitoring tools might be attached with the e-commerce through other means like "Applets: that might monitor and collect individuals browsing habits, secret information like passwords stored through cookies.

B2B Privacy issues:

Unauthorized access to its sensitive information about business's proprietary systems, customer names, operations, pricing and deal terms, financial condition and other competitive transaction information might occurs.

B2C Privacy issues:

<u>Customer perspective</u>: This e-commerce environment is often a "one-way mirror effect". Businesses usually ask customers to provide personal information, but customers have little knowledge about how their information will be used and protected.

<u>Business Perspective</u>: An understanding of customers' privacy concerns is crucial for learning how and what personal information is collected, identify the confidential information and provide solutions to secure each customer's confidential information.

C2C Privacy issues:

C2C websites (ebay.com, amazon.com) enable the sale and purchase of products and services between individual customers. Individual customers frequently buy and sell products and provide private information to complete the transaction. It is the prime responsibility of the C2C e-commerce provider to implement necessary security policies to protect the private information from exchanging between customers and the exchange occurs only under the agreed policies.

Since computers possess the ability to gather and process large amounts of data and the ability of the internet to provide and make available such on a global scale the need and concern for better security has also arisen. In turn consumers, legislators and even privacy advocates have pressed for broader and improved privacy protocols on the interne Grandinetti 1996 and Martin 1973 define Privacy as "the rights of individuals and organizations to determine for themselves when, how and to what extent information about them is to be transmitted to others". Survey results from PolYester Research shows that users belonging to the demographic age of 18 to 24, expressed privacy as the main concern when considering online shopping site. Whilst other research indicated that online users in the US would not register to a website if privacy for a key factor to consider. In order to perform E-commerce activities, a certain amount of personal information is required such as a personal bank account number or an address, when people are concerned about their privacy, they tend to either retreat from performing purchases online or provide incomplete information due to fear. This greatly impairs the further development of e-commerce and affect profits and sales. Recently concluded studies claim 63% of online consumers refuse to provide details due to poor credibility of sites. The success of online transactions therefore is dependent on a strong sense of trust by the consumer. Personal information has always been technically available but its access to the public was limited, the tremendous growth of the internet however simplified the process and now private information can be viewed with a simple mouse click. Andrew Chen, a policy analyst for the Electronic Privacy Centre states that at present, there are no legal guarantees of privacy provided on the web. During the past years, there has been a move from the traditional form of advertising towards behavioural advertising where third party sites track the behaviour of users on first party sites and build up a profile of their interest and activities based on their behaviour. When a user visits a website, a small text file known as a 'cookie' is embedded into their computer, this file acts as a barcode recording or tracking customers behaviour, which pages they visits, which ads they see and for how long. Huge advertising agencies like DoubleClick.com take it a step further, after placing a cookie on a user's computer, these sites can track a user as he leaves a certain website, go to another, and then another, this can all be done without a user even clicking on an ad. Despite the success these marketing strategies are achieving, they also have adverse effects on the success and development of e-commerce. Consumer privacy is replacing theft and fraud as top customer concerns for e-commerce. It was discovered from a study based on tracking and history recording technologies that users showed great concern in terms of privacy on the above mentioned technologies. It is therefore clear the adverse effects that lack of privacy or privacy concerns have on e-commerce success. Companies are advised to tailor solutions to these problems in order to achieve higher market penetration.

Possible Solutions:-

Practical solutions could include developing more customer oriented privacy practices. Introducing a P3P system into company's sites that shows customers how the site collects handles and uses their personal information is also advisable. A recent research suggests that when dealing with e-services, the ease of use of the service and the corporate credibility of the supplier may have a positive influence on privacy risks. Regardless of the methods used, companies must take actions or more precisely increase the quality and amount of measures they provide in order to deliver secure, less risky services to customer.

Non-technical Issues:-

A. Security Awareness:-

Most opinion surveys list "insecurity of financial transactions" and "loss of privacy" among the major impediments to electronic commerce, but in fact most users have only ague ideas about the threats and risks, and a very limited understanding of the technical and legal options for minimizing their risk. As a result all kinds of misperceptions exist.For instance, the cardholder's risk in sending his or her credit card number over the Internet is typically overestimated. At least as of this writing payments over the Internet are treated like mail-order/telephone-order transactions, which means that the cardholder is not liable at all. All risk is with the merchant.

On the other hand, the risks in sending sensitive data in an electronic mail are typically underestimated. Probably most users of email know the mere facts: neither confidentiality nor integrity nor availability is guaranteed. But nevertheless many users do not hesitate to send all kind of very personal and sensitive data to their friends or colleagues, unprotected.

Unfortunately, developers of electronic commerce solutions are often as security unaware and ignorant as their prospective users. For instance, still many developers demand that security must be provided by "lower layers" in a "transparent" way. But, for instance, Secure Socket Layer (SSL) in”opaque socket integration" does not make any sense in most case. Security has to be an integral part of the architecture, design, and implementation.

B. Crypto Regulations:-

Several countries regulate the deployment of strong encryption technology by law. For instance, France controls the domestic use of encryption technology, in order to maintain the capability to eavesdrop on the communication of criminals. The USA prohibits the export of strong encryption products for the mass market, for the same reasons as it controls the export of munitions.

Such regulations do not discriminate between “good” and “bad” applications, and limit the security of honest citizens and companies to at least the same extent as they limit the security of terrorists and organized crime. Therefore several governments, in particular the US administration, are willing to relax their crypto regulations, provided access to the encrypted information would still be possible on demand. The idea is to introduce new “Trusted Third Parties” where secret keys must either be escrowed in advance, or can be recovered afterwards.

All these proposals are still heavily contested, for various technical and political reasons: The Trusted Third Parties would be “single points of failure” for everybody’s, i.e., new and extremely attractive targets for attacks. It is questionable whether any regulation of encryption technology can be effective in fighting organized crime: tools for strong encryption are publicly available, and steganographic techniques can perfectly conceal the fact that cryptographic techniques are applied.

Many types of commercial transactions require strong confidentiality, which cannot be satisfied in some countries, or across some borders. For instance, consider two large companies that prepare a merger. Clearly their negotiations require top confidentiality. Even the fact that they are preparing the merger, i.e., that they acre communicating intensively, will be extremely sensitive. This requires actually services for anonymous communication. Nevertheless using the appropriate cryptographic tools would be illegal in many countries.

Political regulations are not subject to scientific research. But we clearly see the need for an international agreement on a more liberal and consistent regulation of cryptography. Electronic commerce demands strong confidentiality, which can be implemented only by strong encryption schemes.

Legal Issues:-

Surveying the open legal problems in electronic commerce is beyond the scope of this article. The two most important security-related problems are the following:

- Liability: The financial risk of a user in a specific transaction depends on his or her liability. In principle, if a user bears no liability, there is no risk.

  The main issue here is fairness: The liability of a user should correspond to the security of his or her technical equipment. For instance, if it is technically trivial to forge the digital signature of a user then this party should not be held liable for his or her signatures, in general.

- Harmonization: The national laws that regulate electronic commerce over the Internet (like evidential value of digital signatures, consumer protection, copyright protection) are not harmonized, and are partially contradictory. One side result is that there is no mutual recognition between national PKIs, even where comparable laws exist.

Legal Aspects of an E-Commerce:-

The contributions contained in these conference proceedings illustrate how the existing and future regulatory framework for online business transactions works in practice. Various national and international laws. E-commerce presents a world of opportunity for doing businesses, reaching global markets and purchasing without leaving the home or office. E-commerce can provide opportunities to improve business processes, just as phones, faxes and mobile communications have in the past. However, just as any new business tool has associated issues and risks so does e-commerce. It's important to understand the legal issues and potential risks to ensure a safe, secure environment for trading with customers and other businesses. The issue of law on the Internet is a complex one. Between the two all-or-nothing extremes lies a broad spectrum of possibilities. Many people revel in the freedom to express themselves and the freedom from prohibitions such as zoning restrictions that the Internet apparently affords. With no law at all, however, the Internet would be no place to conduct business or pleasure. Laws give people certainties about their rights and responsibilities: they make life more predictable.

The technological basis of e-commerce is basically Web client/server middleware, or what is called three-tier architectures. The client tier is the Web browser involving some type of form processing. The middle tier is the Web server, often with transaction processing. The

Web server in turn links to the third tier, a database processing the order information. Some of the issues are strictly Internet-related, such as domain names and trademarks, linking and framing, click ware (and shrinkware), and metatag use. Others are traditional issues applied to the Internet, such as copyright, contracts, consumer protection, privacy, taxation, regulated industries and jurisdiction. E-commerce site development, its advertising, electronic transaction, money transactions and such involve many legal issues, which need to be taken into account step by step. Before developing an e-commerce site a registered domain and a registered trademark should be established. There must be some copyright protection on the site. The business must ensure that it displays the terms and condition/policies within its site. Security involving the privacy of a user's data is always one of the main concerns while doing business online. Defining rules and regulations for the advertisement of the site by placing banners on other known sites is another. It is of great value when dealing with such complex issues to consult an attorney who specializes in the issues of cyberspace.

CONCLUSION

The research introduced the top two issues in the current e-commerce environment, namely privacy and security issues. These two issues are one of the main reasons to be addressed to further e-commerce development. It elaborated about security issues like identity theft and financial fraud, its effect on e-commerce growth, reasons behind it and the importance of providing secure communication networks in order to attract and successfully retain customers. It also explained privacy issues in e-commerce and the importance of well established privacy settings that ensures confidentiality and safety of customer's information. This was all done in order to facilitate the further expansion and development of e-commerce.

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. So that the e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture.

References

1. Electronic security information centre (http://www.epic.org/security/survey)
2. Electronic privacy information centre (http://www.epic.org/privacy/survey)
3. www.detached.net
4. www.usatoday.com/life/cyber/tech/cth186.htm
5. www.sans.org/dosstep/index.htm
6. http://www.pcworld.com
7. http://www.law.gov.au/www/securitylawHome.nsf
8. http://ecommerce.wipo.int/survey/

All knowledge that the world has ever received comes from the mind; the infinite library of the universe is in our own mind.
~ Swami Vivekananda