Security and Privacy Issues as a Potential Risk for Further E-commerce Development

Rashad Yazdanifard[1], Noor Al-Huda Edres[2] and Arash Pour Seyedi[3]

[1] Faculty of Management, Multimedia University, Cyberjaya, Malaysia - rashadyazdanifard@yahoo.com

[2] Faculty of Business Management & Globalization, Limkokwing University of Creative Technology, Cyberjaya, Malaysia – d@yahoo.com

[3] Faculty of Business Management & Globalization, Limkokwing University of Creative Technology, Cyberjaya, Malaysia – arash_marqhak@yahoo.com

Abstract. E-commerce security and privacy is an important issue that has been leading to negative or adverse effects on the further development and growth of e-commerce. 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.

Keywords: Customer privacy, customer security, e-commerce.

1. Introduction

The utilization of the internet is increasing rapidly every year; availability of low cost peripheral devices and wider internet accessibility options are key contributing factors [1]. The progression of technology over the recent years have enabled the consumer a broader and much more enriched interactive experience.[2] The availability of a wide variety of applications and simple point and click interfaces has further contributed to this “experience” by its ease of usability.

Due to this, IT usage in present times has become a common practice. Business to customer (B2C) transactions and business (B2B) transactions are commonly used in the market. The fusion and integration of these two types of transactions has produced e-commerce [3] [4]. Chen and Dhillon have defined e-commerce as “the transaction of goods and services over the internet “[2]. It is also described as the “sharing, transferring and exchanging of information” [11]. Over the past few years E-commerce has maintained a rapid yet steady pace. It has been a dynamic force, a catalyst in changing the nature of business transactions and operations all around the world [12]. It should also be noted that unlike traditional commerce; EC does not allow physical interaction between the consumers and retailers or suppliers for that matter [2]. This fact raises a number of risks and issues including technological, security, privacy, trust, legal and other related issues [12]. The following research focuses on two of these issues, security and privacy. The factoring of Security and privacy in e-commerce models is of considerable importance to consumers, businesses, and regulators [5]. The majority of customers feel insecure towards the existing policies and guidelines with respect to privacy and security online. Such insecurities have a negative impact upon any economical model. That said, online security breaches can be considered as a fast spreading menace in current day economical settings around the world.

2. Security Issues in E-commerce

In e-commerce development security is a critical factor to consider [13]. 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" [9]. It usually refers to the provision of access control, privacy, confidentiality, integrity, authentication, non-repudiation, availability and effectiveness [12][17][14]. Surveys conducted and compiled recently shows increasing concerns on security risks and have become a global issue [3]. 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 [7].

Electronic commerce has been weakened by the deterioration of confidence held towards it by the consumer public. This in turn poses an immense threat to the overall expansion and success of it. [9]. In fact, Hoffman et al. stated that 63% of online end-users intentionally delay when providing personal information due to diminished confidence and trust in sites [2]. If credibility is to be achieved, improvised security and privacy protocols should be incorporated [6]. At present security is pivotal and concerns surrounding its efficiency is perhaps the key cause for web users not making online purchases [9]. The US-based Better Business Bureau confirmed that online security was a great concern in 2001[2]. Types of security threats include identity theft i.e. the illegal use of personal information and is in fact the USA's leading occurrence of fraud [6] [8]. List of other threats include gaining physical access to premises, accessing wiretaps, unauthorized acquiring of information, viruses, lack of integrity, financial fraud, vandalism, etc [7][12].

Reasons for high security risks include the imperfection of e-commerce laws, regulations, systems, technology and the internet [11]. Security is a key integral issue for users, regardless of what the application maybe, ranging from locking a computer to conducting business via the internet [8]. The rapid development of e-business and e-commerce applications have resulted in increased the amount of illegal infiltration into information systems which were deemed initially safe [3]. Since E-commerce is completely reliant on IT, it could be stated that future developments in e-commerce will solely depend on IT security and risk management [14]. Garg *et al.* states that "a percentage between 36 and 90 percent of organizations confirmed security breaches in the past year alone" [3]. These statistics help increase or maintain customer's negative perception of the e-market and explains why a lot of people are fearful or insecure about buying or performing sensitive transactions online. It seems like the only solution to extract the problem and increase e-sales is to provide fully secured networks that guarantee confidentiality and safety. It is however not that simple. Technologies that provide flawless security measures and guarantees are very expensive and in most cases not easily acquired. Web based e-commerce is compromised of hyperlinked web pages alongside applications and incompatible technologies to bring about business transactions amongst different companies spanning the globe [4]. Therefore, even if a business tries to deploy error free security software, success is not guaranteed as there are many factors influencing the flow and security of information in cyberspace. Moreover, in order for e-commerce to develop customer trust, the change has to be done in a collective manner, not just a few companies. In the case of small to medium businesses it is difficult and costly to incorporate complete IT security [3]. Leaving aside the multifaceted technologies required, e-commerce systems are founded and based on the World Wide Web which coincidently has a history of exposure to a variety of security threats [4]

3. 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 [12][14]. This should change and E-commerce sites should find ways to improve and tailor their security according to customer needs and demands [18]. Software developers must develop software to enhance safety and security and provide safety measures like encryption, digital signatures, biometrics, virus protection, etc [12] [18]. 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. [18]. Therefore, as can be seen, in order for e-commerce security to blossom, it is important to look at it from 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.

4. Privacy Issues

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 [1]. 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" [9]. 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 [1]. Whilst other research indicated that online users in the US would not register to a website if privacy for a key factor to consider [15]. 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[15][16]. 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 [20]

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 [9]. 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 [1]. During the past years, there has been a move from the traditional form of advertising towards behavioral advertising where third party sites track the behavior of users on first party sites and build up a profile of their interest and activities based on their behavior [10]. 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 behavior, which pages they visits, which ads they see and for how long [1]. 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 [1]. 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 [18]. 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 [10]. 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.

5. Possible Solutions

Practical solutions could include developing more customer oriented privacy practices [15]. Introducing a P3P system into company's sites that shows customers how the site collects handles and uses their personal information is also advisable [16]. 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 [5]. 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.

6. Discussion

A review of the impact of security and privacy issues on e-commerce development reveals that with today's rapid growth and expansion of e-commerce, privacy and security concerns are increasing amongst customers. This research unveils how customers' perception of possible risks and threats to the security and privacy of their personal information affects their online purchasing behavior.

Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information.

Therefore, in order for e-commerce to expand and achieve its full potential, companies need to understand these needs collectively try and develop systems, methods or guarantees that would ensure the private and secure communication of information between buyers and sellers. This step would guarantee an increased customer base and eventually prove to be very profitable.

7. 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.

8. References

[1] Mayor.S.Desai, Thomas.C.Richards and Kiran.J.Desai, *E-commerce policies and customer privacy*. Information management and computer security, 2003(11/1).

[2] Bruce Chien-Ta ho and Kok-Boon Oh, *An empirical study of the use of e-security seals in e-commerce*. E-security seals in e-commerce, 2008.

[3] Atul Gupta and Rex Hammond, *Information systems security issues and decisions for small businesses*. IS security issues and decisions 2003.

[4] M.T.Chan and L.F.Kwok, *Integrating security design into the software development process for e-commerce systems*. Information management and computer security, 2001(9/3).

[5] Mauricio. S. Featherman, Anhtony. D. Miyazaki and David. E. Sprott, *Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility*. Journal of services marketing, 2010(24/3).

[6] G.E.Gorman, *who am I, and where's my money?* Issues in online security. Online information review, 2007(31/5).

[7] Someswar Kashe, Sam Ramanujan, Sridhar Nerur, *A framework for analyzing e-commerce security*. Information management and computer security, 2001(10/4).

[8] Norman Desmarais, *Body language*. Library Hi Tech, 2000(18/1).

[9] Godwin. J. Udo, *Privacy and Security*. Information management and computer security, 2001(9/4).

[10] Craig. E. Wills and Mihajlo Zeljkovic, *A personalized approach to web privacy: awareness, attitudes and actions.* Information management and computer security, 2011(19/1).

[11] Xiaoming Meng, *Analyze and prevent the security risks of e-commerce privacy*. International conference on management of e-commerce and e-government, 2008(7/8).

[12] George. S. Oreku, Jianzhong Li, *Rethinking e-commerce security*. CIMGA-IAWTIC, 2005(0/05).

[13] Xin Tian, Wei Dai, *Study on information management and security of e-commerce system*. LEE, 2101. (9/10)

[14] Ralph Holbein, Thomas Gaugler, *IT security in electronic commerce: from cost to value driver*. International Workshop on Database and Expert Systems Applications, 1999. (4/7)

[15] *Internet privacy in E-commerce: framework, review and opportunities for future research*. Proceedings of the 41st Hawaii international conference on system sciences, 2008.

[16] Chunyong Yin, Jianshi Li and Ruxia Sun, *A modified model for private data security facing e-commerce*. Eight ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing, 2007. (7/7)

[17] Licun Wang, Changing Zou, Shubin Zhang, *A study on the commerce security characteristics for electronic business*. International conference one-business and e-government, 2010. (3/10)

[18] Randy.C. Marshani and Joseph .G. Tront, *E-commerce security issues*. Proceedings of the 35th Hawaii international conference on system sciences, 2002. (9/2).

[19] Jeng Chung V.Chen and Yang Ilpark, *Trust and privacy in electronic commerce*. IEEE, 2004. (1/4).

[20] Shouming Chen and Jie Li, *An empirical research on consumer trust in e-commerce*. International symposium on information engineering and electronic commerce, 2009(6/9).