IJITKM Volume 7 • Number 1 • December 2013 pp. 75-80 (ISSN 0973-4414)

Securing E-commerce

Parika Kalra
parikakalra@gmail.com

Abstract: E-commerce has become a critical component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved competitiveness from web-based e-commerce. In this study, we discuss the various models of e-commerce and the need of secure e-commerce transitions. Further we study the different models and methods available for secure e-commerce and Internet risk management system.
Key-words: E-Commerce, CIA Triad model, Internet Risk management.

1.Introduction:

E-commerce provides an important medium for doing business on global based. E-commerce is the electronic automation of business process. E-commerce has become a dynamic force, changing all kinds of business operations world-wide. The related concept and business practices not only influence communication, the routines of daily life and personal relationships, they represent opportunities for initiating new international and domestic business ventures [1]. There are a lot of challenges that have faced by e-commerce. Making of secure transaction on Internet, is really a hard task due to globalization of business through Internet and loopholes that we left remain when making transactions online.

E-commerce has become a critical component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved competitiveness from web-based e-commerce [2]. By doing online business, it is a facility of reaching to everyone. Exploring the opportunities challenges conventional notions of business competition through electronic flows of information and money [6]. Payment on Internet or network is a critical important chain of whole e-commerce, which contains the payment activity. However, though massive manpower and financing are injected into the research of ensuring the safely topic of payment on Internet and E-commerce, yet still many safety problems of financial transaction of E-commerce exists which need to be improved [7].

E-commerce, a subset of e-business, is about the sale and purchase of goods and services by electronic means, particularly over the Internet [4]. On Internet, new forms of currency are using to support electronic payment. Some payment systems involve supporting the existing infrastructure for credit and debit transactions, while other evolving payment system provides payment by means of digital currency [3]. E-commerce is only cannot be defined as doing business or commercial transactions over Internet but it establishes the trust among customers and make a fear-free platform on which a customer can make transactions. It ensures customer for a secure and reliable business transactions. The Internet and e-business are complementary events linked with the progression of related technology [4].

2. E-commerce models:

Basically in the broad terms, there are two types of commerce: traditional commerce and electronic commerce [4]. In traditional commerce money flows by hands of customer and merchant but in electronic commerce means flow of money electronic by using various electronic payment methods.

2.1 Business-to-Business (B2B) model:

Business-to-Business form of e-commerce, is experiencing an explosive growth rate on Internet. Companies of all sizes and types are mutually buying and selling products and services on the Internet. This model provides web-based technologies for all sizes of companies. This offers companies dynamic and exciting business opportunities [5]. B2B also offers unique benefits such as less human intervention, less overhead expenses, fewer inadvertent errors, more efficiency, more advertising exposure, new markets and new physical territories equate to an intelligent method of mutual business. It is a win-win situation for both buyer and seller [14].

2.2 Business-to-Consumer (B2C) model:

Business-to-Consumer form of e-commerce now comes out of its infancy stage. It is basically a concept of online marketing and distributing of products and services over the Internet. It is a natural progression for many retailers or marketer who sells directly to the consumer. The general idea is, if you could reach more

customers, service them better, and make more sales while spending less to do it that would the formula of success for implementing a B2C e-commerce infrastructure [14]. Customer feels more trust on making transactions online. Though consumer continues to experiment online, business-related barriers must still be overcome-security, privacy, uncertainty, low bandwidth, consumer protection and network access [5]. Overcoming to these barriers, B2C become more effective and reliable to consumer. Although consumer and merchant are not face-to-face meet but consumer have more options and have more solutions online.

2.3 Consumer-to-Consumer (C2C) model:
This type of e-commerce is usually a form of an auction site. The consumer lists items for sale with a commercial auction site. Other consumers access the site and place bids on the items. The site then provides a connection between the seller and buyer to complete the transaction. The site provider usually charges a transaction cost. C2C refers a situation where both the seller and the buyer are consumer in an online transaction [4]. Given an individual's lack of knowledge about others selling online as well as the fact that a significant amount of money may be involved in a transaction, a major barrier to C2C e-commerce is likely to be a lack of trust in the seller [8].

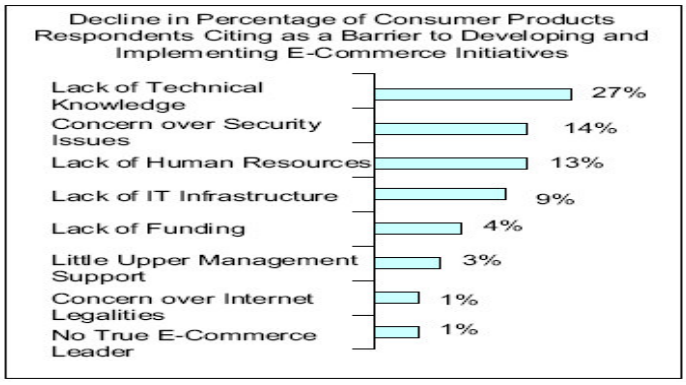
3. Need of secure e-commerce:
There are several reasons why electronic commerce must have stronger requirement on security than traditional form of commerce [12].

3.1 Internetworking of computer systems: Online business has a lot of computer that are interconnected to perform business transactions. Security on each connection requires a deep sight. Secure data and money transfer must be there.

3.2 Data repository: Storage of sensitive data in repositories or databases makes e-commerce system ideal target [10]. Hackers seem any target to data repositories due to availability of data on a single place.

3.3 Lack of forensic evidence: The lack of forensic evidence in computer makes detection, capture and prosecution more difficult [10]. Regular auditing of system is essential for secure transactions.
3.4 No matter of distance: Computer crimes can be committed a thousand of miles from the held place. With the facility of internetworking of system, it is not hard to committing crimes without the barriers of distance and time.

4. E-commerce barriers: There are a lot of factors that prevents our move towards e-commerce. Some of them are [9]:
- Technology
- Security issues
- Lack of trust
- Legal and Regularity issues
- Human resource issues.



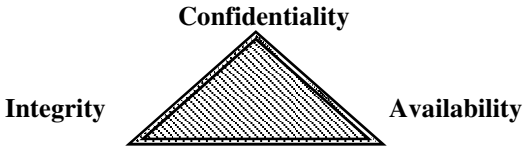
The figure displays the major barriers in the consumer products industry. The survey found that the lack of human resource and the lack of technical knowledge are becoming less of a barrier to developing and implementing e-commerce initiatives in the consumer product industry [9].

4. Security concern to Online Business:

With the increasing speed of Business –to- consumer (B2C) and Business-to-Business(B2B) interactions, accurate and reliable information is essential for online business on the Internet. The major concern must be over the security for make a safe guard for online transactions. E-Commerce can give a company a strong advantage over their competitors while providing greater value and comfort to its customers [1].

4.1 CIA Triad Model of security:

The confidentiality, integrity and availability on the Internet are the basic security concepts [11]. The CIA triad model [13] describes



Information that is read or copied by someone that is not authorized to do so is defined as the loss of confidentiality. There should be a defined level of security access and a depth of information to where a user can get it. Classification of private and sensitive data and information must be made and should not be disclosed. Privacy ensures that customer's data collected from their electronic transactions are protected from indecent and unauthorized disclosure [2]. Information can be hacked from an insecure network and easily modified in a unexpected way, that make a loss of integrity. Integrity ensures that if the context of a message is altered, the receiver can detect it [4]. Availability of information is important to that kind of business that depends on information. Availability ensures that accessed data and computing resources needed by the consumer are reliable, informative and available in timely manner [13]. Including these, there are some more factors that needed in security such as: (a) authorization (b) authentication and (c) non-repudiation.

5. Security by Depth:

Security can be defined as term in which the information or data is stored in the system cannot be read or compromised by unauthorized users. "Bad people do bed things." Jeff Mallet, president of Yahoo!, Inc. made that observation in the aftermath of the recent "hacker attack" that sent the world's largest electronic commerce sites reeling [16].

Threats to security:

The online consumer uses the web browser as front- end to make a transaction. Web browser poses risks to the user's security and privacy of the information. The more risk arises when a user visits unknown web links that are un trusted, having the lack of knowledge of these links. Sometimes uploading or downloading of files may cause to make a loophole for secure user systems.

Cookies are another web technology that can be used to hack the end users' privacy. Cookies are data that are sent back and forth between the web server and client to maintain state between Web connections. Web server uses this information to know about the browsing habit of the user and displays these kinds of links without the permission of the user.

Some **Active X controls** are placed on the webpage to download the information about the system configurations by downloading itself to user's machine and after reading its mail files send this information back to the Web server. The notorious Computer Chaos Club out of Germany demonstrate the ability to download a seemingly ActiveX control that in fact scheduled electronic transfer of funds from the users' account to a numbered Swiss bank account [17].

Java Applets automatically downloaded from any Web page and run within the user's Web browser. Java Applets gain access to sensitive files on the users' desktop. Java Applets are considered un-trusted code that must be carefully handled.

Moreover there are other kinds of threats with concern to e-commerce security as (a) Unauthorized access (b) Malicious code (c) Financial Fraud such as credit card fraud etc.(d) Denial-of-Service attacks [9].

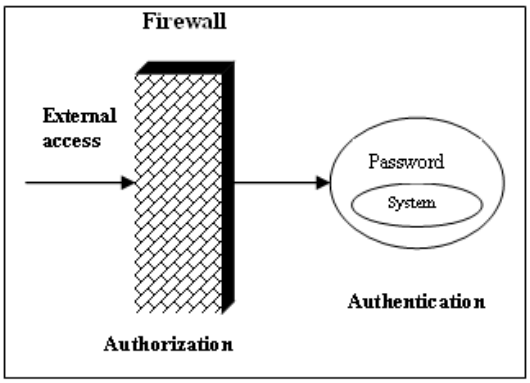
6. Security solutions:

We can classified various technologies that are used to prevent from stealing the confidential information in online business [9] :

(a) Cryptographic technologies
(b) Access Control and authentication protection
(c) Virus protection tools
(d) Other combination of technologies
(e)

Cryptographic Technologies: Cryptology uses the techniques in which the plain text information is converted in cipher text using various schemes and methods that cannot be read even if the information is hacked. We used various encryption schemes, digital signatures, Hash function and digital certificates [9].

Access Control and authentication protection: There must be a level of information on that the user can access the information. Boundaries to the information must be defined. If there is access control the most of attacks are impossible. Firewall can be used for this kind of access controls. Setting the password to sensitive information can protect the data. Password used after the hacker cross the Firewall or authorization but kept in authentication.



Biometrics can also be used with concern to identifying a person based on his or her physiological or behavioral characteristics. Biometrics are utilized for authentication and as a result, protects confidentiality and integrity [9].

Virus protection tools:

Today, there are various kinds of anti-virus and content-filtering software introduced in the market. There are five distinct methods identified for fighting against viruses [9]:-

- Signature scanning anti-virus software
- Integrity checking anti-virus software
- Heuristic anti-virus software
- Macro virus analyzers
- Polymorphic virus analyzers

Other combination of Technologies:

Including these protection schemes, some protocols are also used for secure the sensitive information as Secure Socket Layer (SSL), SET, PGP, Secure Hyper Text Transmission Protocol(S-HTTP), Secure MIME(S/MIME) etc.

7. Internet Risk Security Management:

Business must determine the themes that are most valuable for them. It must be planed to put them together, planned and implement the plan. Risk management consist of four phases-assessment, planning, implementation and monitoring [1]. During the assessment phase, the organization estimated the security risk. It contains five steps. First is to establish the objectives of an organization. Second is assets inventory that is to define the tangible and intangible assets. Third step is to delineate threats in which we find out the origin of threat. The next step is identifying vulnerabilities. Various tools and methods are used to find out the weakness of network. The final step is to quantify the value of each risk by assigns a value to each risk [1].
The second phase is planning. In planning, sets of security policies define which threats are tolerable and which are not. By means of tolerable threats that have less risk in network. This phase also have some steps. In first step specifies the policies. Second is establishing processes for auditing and review [1]. Review is needed to check the effectiveness of policies. And last step is to make the final plan that will be implemented on network. The third phase is the implementation of the plan. Technologies are chosen as defined in planning phase. The last phase is monitoring. Monitoring is a continual process that aides in the determination of which technologies are successful, which are unsuccessful and need modification, whether there are any new threat [1].

Conclusions:

E-Commerce is the developing trend of the economic development. Network payment relies on the establishment and completeness of electronic online safe trading. A secure online transaction requires a lot of security concerns. E-commerce is still very much in an experimental phase. Basically there are many solutions that are available for secure Internet business but still have to wait for its best use. The basic is to prevent the messages (payment, order) when there are a lot of barriers due to broad network. This paper does not provide the efficient solution for secure E-commerce but it explores the tools and methods that may be used to make secure, trustful and reliable online business. A safe e-commerce environment made it easy to establish the trust of customer. Overall E-commerce sites need to be concerned with the variety of security issues including: authentication-verifying the participants that are involved in the transactions; authorization-verifying the user has permission to specific data. Security becomes the most essential concept in E-commerce and still have more to explore the security weak links.

References:

[1]. Bob Gehling, David Stankard “eCommerce Security”, Information security curriculum development Proceedings of the 2nd annual conference on Information security curriculum development, 2005, P: 32 - 37
[2]. P.Ratanshigham “Trust in Web-based Commerce Security”, Information Management and Computer Security, 1998 vol.6,no.4.p162-166.
[3]. A.K.Gosh, ”E-Commerce security: Weak links, Best Defenses”, John Wiley & Sons, New York NY, 1998 ISBN-0-47-1922-3-6.
[4]. H.Chan, E T Al “E-Commerce”, Chichester, Wiley 2001.
[5]. T.Colman, ET Al “Keeping E-Business in perspective”, Communication of ACM, August,2002 vol.45. no.8 page 69-73.
[6]. X.Sahi and P.C. Wright, “ E-Commercializing Business Operations” Communication of ACM, Feburary,2003 vol.46. no.2 page 83-87.
[7]. Ji Zaho, “Security Research on Payment System on E-Commerce Network.”
[8]. T.J. Strader and S.N. Ramaswami, “The value of seller trustworthiness in C2C online markets”. Communication of ACM, December,2002 vol.45. no.12 page 45-49.
[9]. Chander Kant, Rajender Nath "Off-line Optical Frustrated Total Internal Reflection" Published in the proceedings of National Seminar on “Information and Communication Technology- Recent Advances & Applications ICT-2006 PP 237-240 Feb 09-11, 2006 at JMIT, Radaur Yamuna Nagar
[10]. Anup K. Ghosh “E-Commerce security: No Silver Bullet” IFIP Conference Proceedings; Vol. 142, P: 3 – 16, 1998
[11]. Dekker, M,(1997) The Frorlich/ Kent Encyclopedia of Telecommunications vol.15. NY p.123
[12]. G.W.Treese “Inernet Security: To worry or not to worry? EDI Forum Journal of Electronic commerce 10(4): 54-58,1997
[13]. C.Barnes, ET Al “Hack proofing your wireless networks” Syngress Publishing, RockLand, MA,2002.
[14].http://www.isos.com.my/ecommerce/b2b.htm

[15]. Anonymous (2003) Special Report.2003 April 17. Computing; security; smart moves to earn consumer confidence retrieved July19, 2003 from Lexis Nexis.
[16]. Zinkewiez Phil 2000, Feb19, Insurance Advocate.Hacker Attackers Raise troubling questions on e-commerce Security Developments.
[17].Klaus Brunnstein, Hostile ActiveX control demonstrate RISK Digest 18(82), February 1997.