A CONCEPTUAL REVIEW ON CHALLENGES AND SECURITY ISSUES IN E-COMMERCE

Mrs. Vinutha H. K. [1]
Ms. Shilpa K. [2]

Abstract:

E-commerce is the process of buying and selling of various products and services by businesses through the internet. E-commerce is the web to conduct business but when we concentrate on commercial deals among organizations and individuals demanding selective information systems under the guarantee of the firm it accepts the form of e-business. It encompasses the entire scope of online product and service sales from start to finish. E-commerce tools include computer platforms, applications, solutions, servers and various software formats manufactured byE-commerce service providers and purchased by merchants to increase online sales.

Without proper security measures in place, e business are at risk of losing customer's data and revenue. Security risks associated with E-commerce can be as a result of human error, an accident or unauthorized access to systems. Security issues in E-commerce such as integrity, authentication and non-repudiation must be dealt with effectively for any online business to be successful. To solve the security issues in E-commerce, merchants and payment companies should collaboratively come up with effective solutions.

Key Words : *E-commerce, Cyber Crimes, Web-site, Data-base, Internet, Hackers*

I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image. - Stephen Hawking

Introduction:

The cutting edge for business today is E-commerce. Today E-commerce is a by-word in Indian society and it has become an integral part of our daily life. E-commerce stands for electronic commerce. It means dealing in goods and services through the electronic media and internet. On the internet, it relates to a website of the vendor, who sells products or services directly to the customer from the portal using a digital shopping cart or digital shopping basket system and allows payment through credit card, debit card or electronic fund transfer payments. E-commerce involves carrying on a business with the help of the internet and by using the information technology like electronic data interchange. More simply put, E-commerce is the movement of business onto the worldwide web.

Objectives:

- To study the existing security threats involved in E-commerce.
- To carry out an intensive study on dangers & threats created in the usage of E-commerce practices.
- To understand various derivational damages & side effects caused due to E-commerce applications.
- To forecast & predict subsequent potential impacts that may be newly crept into the system out of the addiction to the technology.
- To suggest suitable measures to take care of security issues.

[1] Assistant Professor, Department of Commerce , Sri Mahaveera College, Moodabidri

[2] Research Scholar and Lecturer, Department of Commerce, Sri Mahaveera College, Moodabidri

Methodology

The data have been collected and analyzed in the study from secondary published sources viz., books, newspapers, websites and research studies. The proposed study is confined to discuss the security issues involved in E-commerce.Cybercrimes, online identity verification, Omni channel customer experience, data leakage, records maintenance, phishing, bank information stealing, ethical hackers, identity theft, credit card stealing are some of the variables that are discussed in the paper.

Review of Literture

Raven, compared India and china's approaches in adoption of E-business. Based on the literature survey and secondary data, the study analyzed various factors influencing the growth of E-business in the two countries. The factors examined include government policy and focus, existing technology infrastructure regulatory environment, experience and understanding of business operations, and culture, among others. The study concludes that china appears to be ahead of India in the infrastructure, but India is ahead in E-readiness. Further, in states that both countries are poised for rapidly increasing E-business. However, problems of poverty and inequality between urban and rural connectivity must be resolved to really take advantage of E-business in both the countries.

Miyazaki and Fernandez (2001) stated that information privacy and security would be the major obstacles in the development of consumer-related e-commerce. They described that risk perceptions regarding Internet privacy and security have been identified as issues for the consumers. They explained that the early research suggested that the risk perception wouldn't affect e-commerce much. However, recent studies revealed that consumer risk perceptions would be the main obstacle to the growth of E-commerce. They explained that the higher Internet experience would reduce the risk perception of E-commerce which includes system security, retailer fraud and privacy. They suggested that further research is needed to find out how risk perceptions influence e-commerce, how retailers should manage it and how the management of risk perceptions may impact consumer welfare. These are the limitations of this article.

McKeefry (1998) stated at the beginning of the E-commerce, consumers were concerned about the credit-card information they released over the Internet. However, now many of these concerns have been solved by the integrators and developers and thus, produced a secure environment. In fact, educating the consumers about the security of Internet credit-card transaction is more important. They explained that SET (Secure Electronic Transaction) is one of the solutions for the security issue in E-commerce especially in credit-card transactions. It is expected to cover other payment methods in the future. The limitation of this article is that it didn't explain in detail about how to educate consumers about security of Internet credit-card transactions. Besides that, discussion about transactions in e-commerce in this article is limited to credit-card transactions only.

Chadwick (2001) stated that creating trust is one of the processes in building a relationship with a consumer. He mentioned that research showed that trust could develop over timeor swiftly. He explained that there is a difference between E-commerce interactions and face-to-face interactions in the process of building relationship with a consumer. He stated that trust must exist for a successful transaction. He described that trust does affect how consumer can behaves in an E-commerce transaction. When the price differences are small, consumers preferred to buy from an online company they trust. He also explained that trust problem appeared both in E-businesses and consumers.

Website in E-Commerce

For choosing an E-commerce Web Development Company, there are some factors that need to be considered for good business. The most important factors which must be analyzed are the capabilities, creativity, and specialization of the company and it must be reviewed time to time which helps in selecting better options for the business development. Some of the points which need to be checked before making a decision to select an E-commerce development company are:

- ***Availability of Staff*** : The company must have high skilled, experienced & professional enough number of staff available with them to handle & manage your project properly. There should be few account managers assigned to your company to handle & address your queries & concerns.

- ***Deep Knowledge :*** The team responsible for design & development of the website or portal must be well versed with networking, latest technology, programming, software development & SEO tactics to create a user friendly & SEO friendly website.

- ***Responsible :*** Besides having sound and versed workers, the company must have an ability to take the responsibility of the client, by keeping in mind about the client's requirements. So it is important to check its credibility by previous clients.

- ***Delivery of Product*** : There must be a proper and on-time delivery of the products, in order to maintain the long relationship with their clients and make them happy at all times. So punctuality & timeliness of the company needs to be checked.

- ***Is E-commerce Important for the Business? :*** E-commerce business is the best option available for the people to build a better business world for insuring success in future rather than doing a traditional mode of business. For any business person, to have an E-commerce business is added advantage for their business.

Emerging E- Commerce Threats

- E-Commerce business is all about the right execution. The online store should offer a good shopping experience to the users. Customer satisfaction becomes an important factor to make your E-Commerce business successful.

- E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. It includes:

- ***Omni Channel Experie***nce : Lack of transparency of inventory across the enterprise, and navigating each and every customer uniquely are the biggest challenge for retailers in implementing omnichannel.

- Data SecurityAttackers can not only infect website with viruses, but they can also expose confidential data.

- ***Online Credit Card Fraud:***

- When an Internet vendor detects fraudulent credit card information, the credit card cannot be confiscated and the fraudster and credit card are free to try alternative sites.

- Fraud perpetrators are also free to use stolen card numbers or even attempt to manufacture numbers for use, as purchase over the Internet does not need the actual cards and signature.

- The remoteness of the buyer and seller make it extremely difficult to apprehend the fraud perpetrator. In fact, remoteness is among the factors that attract individuals to Electronic commerce fraud.

- ***Privacy :*** ID numbers, passwords, credit card numbers and fraud instruction guides are available in Internet chat rooms. Applications Corp claims that many Electronic commerce sites do not adequately protect consumers databases and are vulnerable to hackers seeking customer information.

- Competitors are a real hazard to companies engaging in Electronic commerce as they try to steal valuable customer information. Thus, key passwords for sensitive directories are likely to be broadcast semi publicly over the Internet, where anyone with a little luck and packet sniffer can discover them.

- ***Domain Name System (DNS) spoofing***: Hackers with write access changes the translation file rerouting web surfers to hacker.com. If the two webpage's look identical, even prudent customers can be easily defrauded and the company's reputation damaged.

- ***Vulnerabilities in General Security Procedures:***Carelessness like giving out passwords over the phone, or throwing security manuals without shredding can create problems if it falls in the wrong hand.

- Spamming: It means 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.

Cases of cyber crimes caught and handled in India:

Sl. No.	Crime head	2010	2011	2012	2013	2014
1	Tampering computer source documents	64	94	161	137	89
2	Computer related offence	510	983	1875	2516	5553
3	Transmission in electronic form	328	496	589	1203	758
4	Unauthorized access to protected computer system	3	5	3	27	0
5	Obtaining digital signature certificate by misrepresentation	9	6	6	12	5
6	Publishing false digital signature certificates	2	3	1	4	0
7	Fraud digital signature certificate	3	12	10	71	3
8	Breach of privacy	15	26	46	93	18

Types of web crimes:

Cyber crimes	Hackers	DOS (Denial of Service)
Online credit card frauds	White hat hackers	Spamming
Privacy	Black hat hackers	E-mail bombing
DNS	Grey hat hackers	Surfing
Masquerading or spoofing	Red hat hackers	DDOS (distributed denial of service attacks)
Sniffers	Blue hat hackers	Viruses
Theft of software	Elite hackers	Worms
Theft of hardware	Hacktivist	Trojan Horses
Passive unauthorized access		
Active unauthorized access		

Preventive Measures

A few technology methods to overcome the security threats are listed below:

● ***Encryption :*** Sensitive information such as credit card details can be defended by encryption, that is, the use of secret codes. The goal of encryption is to make it impossible for a hacker who obtains the cyphertext (unreadable form of the message after being encrypted) as it passes through the network, to recover the original message.

There are two main types of encryption:

- symmetric or private key systems.
- asymmetric or public key systems.

In a Privatekey system, the same key is used to encrypt and decrypt the plaintext. The key is called a private key and must be shared by the sender and receiver of the text.

● The private key must be kept confidential, and must be known only to its owner.

Public-key encryption uses two closely related keys. One key is used to encrypt the message, and the other key is used to decrypt the message. The public key can be made known to other parties, and can be distributed freely both keys, however, need to be protected against the slightest modification, or the mechanism will not work

● ***Digital Signature :*** A digital signature is a cryptographic method that fulfills a similar purpose, as does a written signature. It is used to identify and verify the originator and the contents of a message. That is, a recipient of data (such as an email message) can verify who signed the data, and that the data was not modified after being signed. The main purpose of digital signatures is for sender authentication.

● ***Digital Certificate*** : Authentication is further strengthened by the use of digital certificates. Digital certificates verify that the holder of a public and private key is who they claim to be. Third parties called certificate authorities (CA) issue digital certificates. A certificate contains items such as the subject's name (owner of the private key), validity period, subject's public key information and a signed hash of the certificate data (i.e. hashed contents of the certificate signed with the CA's private key). Certificates are used to authenticate Web sites (site certificates), individuals (personal certificates) and software companies (software publisher certificates).

- ***Secure Socket Layer (SSL):*** It addresses some of the security concerns relating to data transfer over the Web. The Web itself, because it uses simple TCP (Transmission Control Protocol) for its transmission process, does not encrypt the data sent across it. Anyone who intercepts a Web transmission has complete access to the data contained therein. If a transmission containing credit card numbers falls into the wrong hands, it is important that this data should not be readable by anyone other than the sender and the intended recipient.

- ***Secure Electronic Transaction (SET)*** : It is developed by Visa and Master/Card. There are 3 entities in a SET transaction -customer, merchant and payment processing firm. SET use SET digital certificates for each of these entities to ensure mutual authentication. When a customer wants to make a purchase, he uses an electronic wallet. An E-wallet is a helper application used to store information about the customer's credit cards and the SET digital certificates for each of the cards. The E-wallet sends both the order information and the payment.

Suggestions

- Adoption of safer online payment system.
- One-click checkout can help to prevent cart abandonment. Allow the customers to save the information and other details for a faster checkout.
- A natural, balanced spread of opinions can attract the users and they may be able to show trust in any brand.
- Avoid any suspicious reviews or fake reviews on website.
- Consumers must educate themselves to protect their confidential information and consumer rights.
- There are many passwords guessing programs publicly available with built in dictionaries containing hundreds and thousands of words so users must be careful.
- Consumers should be more proactive to know the sites they are visiting and be more cautious in giving personal or financial information and also take the effort to know the credibility of the organization they are dealing with.
- Internet Security and Consumer Rights courses are to be made available in secondary education system. Citizens should be taught about these issues when they are young.
- IT and Internet Security Road shows and Exhibitions to be extended to rural areas to educate the rural people.
- Educate consumers as to how their personal data can be protected.

Conclusion

E-commerce is not just about setting up a website and selling online, it is much more than that. It takes a diligence, hard work, persistence and mostly, the courage to take risks. The dynamics of the electronic commerce industry are continuously changing depending on the customer's demand and shopping behaviors. E-commerce business provider should give importance on every customer by giving smooth service and many options for payment and have more functions available online. The role of government is to provide a legal framework for E-commerce so that while domestic and international trade are allowed to expand their horizons, basic rights such as privacy, intellectual property, prevention of fraud, consumer protection all are taken care of.

❊ ❊ ❊ ❊ ❊

REFERENCES

" ISSN (Print): 2319-5940 ISSN (Online) : 2278-1021 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.

" International Business & Economics Research Journal Volume 3, Number 9 Reviewof E-Commerce Issues: Consumer's Perception On Security And Privacy SaravananMuthaiyah.

" Sri Rama college of commerce, university of Delhi, paper CH 6.3(B) Chakravarthy, K.D Chatterjee D, E-commerce B.B kundu, grandson, KolKatta (2011 pp.22.5).

" Global journal of management & Business research, volume 16, Issue ISSN 2249 4558. Scholar issues for inter disciplinary, ISSN -2278888. Development of e-commerce technology E-com practices respects, Dr. Ravj, ISSN: 2319 - 9202.

" Arpana, & Chauhan, M. (2012). Preventing Cyber Crime: A Study Rrgarding Awareness of Cyber Crime in Tricity. 2(1).

" Dalla, H. S., &Geeta. (2013). Cyber Crime - A Threat to Persons, Property,Government and Societies. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), 997-1002.

" Julka, H. (2015, Nov 20). What ecommerce companies like Flipkart, Snapdeal, Uber are doing to battle fraud. India. Retrieved Feb 5, 2016, from http://articles.economictimes.indiatimes.com/2015 20/news/68440486_1_flipkartsatinder-singh-drivers.

" Shrivastav, A. K., & Dr. Ekta. (2013, July). ICT Penetration and Cybercrime in India: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 3(7), 414-419.

" David J. Olkowski, Jr., "Information Security Issues in E- Commerce", SANS GIAC Security Essentials, March 26,2001.

" A.Coulibaly&A.Inam."SecurityIssuesFacingE-Commerece", From Internet http://WWW.ACM.COM.

" Brian McWilliams and Clint Boulton,"Another E- Commerce SiteSuffers Hack Attack", intermetnews.com, March 2,2000.

" E-Commerce site security,http://www.applicure.com/solutions/eco e-commerce security