Pacific Business Review International
Volume 7, Issue 4, October 2014

Hacking and E-Commerce: A Review with special reference to India Act 2000

Anand Vyas
Research Scholar
School of Management
JECRC University, Jaipur

Dr. Sachin Gupta
Assistant Professor
School of Management
JECRC University, Jaipur

Abstract

The purpose of this research paper is to identify how much hacking is affecting the E-commerce transactions in India. The significant growth of E-commerce market is remarkable in India. More and more consumersare transferring to E-commerce to achieve better and fast transaction. Hacking is become vital problem for E-commerce user. Lack of knowledge and ignorance of proper security mechanism over internet cause lots of hacking cases in India. Information Technology act 2000 play a vital role for revocation of hacking in India. This research paper identifies the factors affecting the hacking on E-commerce transition in India and How the IT Act 2000 still bound those factors. This research paper's theoretical contribution is to explain that 'How's IT Act 2000, helps India for growth of E-commerce industry and provides safe and better online transaction.

Keywords:

E-commerce, hacking, Information Technology act 2000, India.

Introduction

E-commerce refers to the use of electronic mean and technology to conduct commerce. Althoughits refers to paperless exchange of business information using electronic data interchange and electronic fund transfer. E-commerce infrastructure includes computer and internet penetration, quality, speed of the internet connectivity, existence of security infrastructure and online payment mechanism.

So we can say that E-commerce is an emerging business concept in India. India is the second largest market in Asia, Nowadays in a developing nation E-commerce is a basic need for rapid growth in economy. It pertains to a website, which sells products or services directly from the site using a shopping cart or shopping basket system and allows payments through cards, e-banking, cash on delivery.

Hacking

Computer hacking is generally defined as purposely accesses a computer without authorization or exceeds authorized access. Various authors define hacking in many ways but common and universally adopted definitions are as follows:

1. Whoever -

1. Having intentionally accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the IT act 2000,
2. Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
   - A. Information contained in a financial record of a financial institution, or of a card issuer or contained in a file of a consumer reporting agency on a consumer.
   - B. Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.

Objectives

- ➢ To analysis the security level of E-commerce transactions in India.
- ➢ To analysis impact of IT act amendment 2008 over the E-commerce transaction.
- ➢ To find out the spectrum of E-commerce in India and how it is affected by IT act 2000.
- ➢ To find out how much IT act 2000 effective for revoke of hacking in India?

Scope

Research area mainly focuses upon E-commerce transaction and hacking in India. Research is emphasized upon what difficulties are being faced by user for doing E-commerce transactions and how they can be beware of fraudulent websites. Research paper also gives stress in finding out the security level of E-commerce transaction in India.

Spectrum of Security level of E-commerce in India

The IT act 2000 also needs the use of material security actions, which it defines as practices and procedures intended to protect sensitive personal information from unlawful access, damage, use, modification, disclosure or impairment. In the absence of an agreement or law, reasonable security practices may be prescribed by the Indian Central Government. Although this provides little clarity in describing the practices and procedures required.

We have to consider all these areas in order to find solutions for E-Commerce security. This research investigates the major factors that influence the type of external Security measures required and implemented by an organization. Factors include: technical, reputation, societal, legal, and management factors. Security spectrumincluded interaction of users, hardware, and software. A noble security system should not only look at hardware and software, itshould also cover other areas such as physical security, human security, business and disaster protection, and legal implications. Because of the astounding nature of E-Commerce, we need to mention all security issues. For example, Government can provide good network security but it might depend on the particular country's encryption rules.The paper reveals that the past IT Act is weak on various fronts and in the absence of sound legal framework E-commerce cannot create a success story in India.

There are many important issues which are material for the success of E-commerce that have not been covered or appropriately addressed by IT Act. Indian Government must participate for the safe and secure business spectrum on cyberspace, a healthy legal framework will be establish for benefits of E-commerce industry.**Sections 69 through 69B** grants to the Central Government the authority to intercept, monitor and block access to electronic information in the interest of national security, and to monitor and collect traffic data (data identifying a person, computer system, or location to or from which the communication was transmitted, including origin, destination and other details) for purposes of enhancing cyber security, all in accordance with procedures and safeguards as may be prescribed.**The Ministry of Communications & Information Technology** has posted draft rules prescribing such procedures and safeguards at its website for public comment. Among other things, the draft rules require authorities to consider whether there are other ways to acquire the necessary information and to issue orders to monitor or intercept such information only if it is not possible to obtain the information by other reasonable means. The draft rules also place time limits on how long an interception or monitoring order may remain in force, how quickly intermediaries must respond to an order for monitoring or interception of information and how long security agencies and intermediaries may retain the information obtained.

Section 70B creates a government agency, dubbed the Indian Computer Emergency Response Team, with responsibility over the analysis and dissemination of information and alerts regarding cyber incidents, the coordination of responses to cyber incidents and the issuance of guidelines regarding information security practices and the prevention, response and reporting of cyber incidents. This paper suggests that there are still lot of work needed for upliftment for Indian cyber laws and regulations.

Significance

Significance of research paper can be divided into two parts. First is for E-commerce user, it helps to understand more intensely that what are the threats being faced for doing E-commerce transaction. Second for government to analysis loopholes in security of E-commerce transactions and how these factors can be eliminated by making rules and regulations for more secure and safe online transactions in India.

Findings

Still there is a lot of work, which is to be done for safe and secure transaction of E-commerce. We just keep in mind that E-commerce is a new Industry in India. Still computer literacy level is low in India. Still cyber threats are not apprehend by entire population. These industries see an astounding rate of growth. E-commerce market grows in India because so many growth drivers are favorable in India such as changing youth's perception, introduction of trusteeship model, growth of financial area and number of smart phone buyers is increasing. But still so many threats exist in an Indian E-commerce market which is going to be solved by Indian Government with the help of strict cyber laws and regulations.

Suggestions

Indian government should take necessary steps to reduce cyber threats in India by making strict rules and regulation against them, provide awareness and literate more people for cybercrimes and frauds and safe and secure E-commerce uses. Some rules and regulations should also be changed for revoking cyber threats. At last but not the least, we conclude that since E-commerce industry is not new in India, because of this, there are so many fears, threats,challenges, gaps, hurdles and obstacles are in front of the industry as well as for users. If this problem can be managed then an upliftment of an Indian economy is possible.

Limitations

Certain limitations were recognized while interpreting the findings. First, these studies only focus on hacking on E-commerce transactions while other types of cybercrimes like key logging, phishing etc. were ignored. Second, the Indian online market is huge; many loopholes are still not recognized in an Indian E-commerce market security mechanism.

References

Bajaj K.K., Nag D., Bajaj K. K.,(2005). Ecommerce, Tata McGraw-Hill Education.

Change K.C., Jackson J., Grover V.,(2003). E-commerce and Corporate Strategy: An Executive Perspective, Information & Management, 40, 663–675.

Deshmukh S., Deshmukh P., Thampi G.T., (2013). Transformation from E-commerce to M-commerce in Indian Context,International Journal of Computer Science, 10(4), 55-60.

Duggal P., (2002), Business & Economics , Saakshar Law Publications.

Hassan A.A., Pons A., Collins D.,(2003).Global E-Commerce: A Framework for Understanding and Overcoming the Trust Barrier. Information Management & Computer security, 11(3), 130-138,

Kamel S.,(2006).Electronic Business in Developing Countries Opportunities and Challenges, Idea Group Inc.

Manjoor A., (2010).E-commerce, Amir Manzoor, 02.

Mcknight D.H., Chervany N. L, (2002). What Trust Means In E-commerce Customer Relationships: An Interdisciplinary Conceptual Typology, International Journal of Electronic Commerce/Winter, 6(2), 35–59.

Mittal D. P., (2000).Computer networksIndia Taxmann Allied Services.

Nariya H., Gohel C., (2012). E-Commerce System: A Review on Security Challenges and Indian Perspective, Journal of Information, Knowledge and Research in Computer Engineering, 451-457 2(2).

Udapudi V.S., Ghosh B., (2012). The Information Technology Act of India: A Critique, Zenith International Journal of Business Economics & Management Research, 2(5), 182-194.