Original Research Paper Law

Cyber Security in E-Commerce

Dr. Anjani Sigh Tomar | Asso. Professor of Law Gujarat National Law University Gandhinagar

ABSTRACT

India is ranked as the country with second largest user base of e-commerce in the entire world after China. It is also predicted that after few years down the line India may be the largest e-commerce market of world. With so much of growing e-trading in India, it not only requires mutual faith among the parties but is so need that there must be data security & protection. As it could be well understood that the e-commerce do require the monetary transactions & without the faith in the e-transactions this could not be met out. Variously we have seen that there are instance of the breach of the security & also the websites are hijacked. This is not only happening in India but also in the developed countries too & seen many examples in which the intruders could also breach the firewalls of the top institutes of world. The transactions during e-commerce is mostly through the intermediaries, whose role is very significant. Previously in India when there is no law pertaining to these aspects the situation was very bleak. But now we have framed the law & also the rules associated with it. Now we have fixed the liability of not only the banks but also that of the intermediaries.

Present paper is aiming to bring out various aspects of the e-commerce, the stages of the major types of transactions, the security issues with it & the available remedies with application of law. This will be concluded with suggestions. The various stages of the e-commerce include the formation of the contract & passing the consideration through the e- means. Now as the transactions are commonly through e-means it becomes imperative that one must know that at which stage the violations are maximum, or possibilities of the breach are highest.

KEYWORDS E-commerce, Cyber security, Information Technology.

Introduction: Cyber security is very debatable & discussed issue these days. This is because of simple reason that all of us are dependent on internet in one or the other way. If not doing the commercial transactions, we are involved in e-banking or e-ticket booking which also require the secure mans in every transactions. All the official work is with the computers only, hence we require the cyber security in every possible manner.

Objectives: The present paper will bring our measures to protect your transactions in e- medium. The possible suggestions will be offered by the authors which may help to contain these matters in timely manner. To create awareness is also an objective for said paper.

Research Methodology: This is primarily the doctrinal methodology which was based on the articles & comments written by the various authors.

Literature Review: The book written by Ms. Karnika Seth, 'Computer, Internet & New Technology Laws has relied to cover issues of cyber security.

A book by Justice Yatinder Singh on Information Technology Law was also referred to understand the issues in security at internet use.

Cyber Security:

Cyberspace is that virtual place where no boundaries exist, no law is concrete but which has become all & all omnipotent & inevitable for humans. E-commerce as we know it today was started in year 1979 when Michael Aldrich has created this idea turning into reality. The initial aspects only involve a medium for interaction but today it has grown to a level that it is a giant intermediary which is regulating all of us in one or the other way. Cyberspace is now the most important way to do business, and also to show the presence of one at Global level. It plays a very pivotal role in fulfilling all the essentials of an easy market. Looking to the facts, India is one of largest growing e-market of the world. If we compare that with size the e-commerce market in India has shown sharp growth rate in 2014. With the advent of the smart phones, and apps on them have actually made the entire e-commerce a different thing. If we go by the data it was found that persons of young age in India are the maximum buyers online where the sale was done on the apps through mobile phones. Year 2014 has also seen a raise of more than 30% in total e-commerce done in India and it was projected that year 2016 will further set new heights for the ease of sale & purchase.

The elements of e-commerce not only include the sale & purchase only, but it also include the bank transactions done by us & by banks in day to day life. The e-transactions done for the sake of doing business also amounts to e-commerce. Recently we have seen that e-payment companies like Paytm has also operating as virtual banks , similarly there are all major banks offering portals for net –banking which again means the actions in e-commerce.

Let's examine what are the reasons of the growth of e-commerce in India:

1. Easily available goods: Today everyone wants to save time, because of the multitasking one is forced to do. Which means that curtailment of some time for some activities. The e-commerce is a medium or big market where the things are available at your disposal. So there is preference for this.

2. Young population in India: Today India is supporting largest young population of the globe, which is energetic & ready to take risks. Hence they prefer the excitement of the e-purchase. Also they have a connectivity through internet, which propels them to do things at par with their counterparts in western countries.

3. Cheap but standard goods online: Many Indians prefer goods online due to the cheap price with no compromise with standards. Since it is a good option available. Most Indians are promoted to take up e-marketing. The offers which the offline markets are providing is very less as compared to online markets, and their ingress is also more due to increase use of Internet, hence they are most preferred.

4. Increase in pocket power & small size of families is also a major reason behind hype in e-retailing. On an average India have witnessed a steep fall in the size of families with increase in pocket powers, which means more of trade possibilities. This has also promoted many of us to do transactions online.

What is cyber security: As it could be easily understood that cyberspace is very vulnerable in itself, it has been seen that there is threat to everything kept in cyberspace, be it data or network or any other thing available at online medium. The threat is not only limited to the financial information, but even the stored data on computer can also be subject to attack by people who are only interested to damage the property. The threats at cyberspace are huge, from financial losses to the loosing data, loss of privacy & of course the social image loss. The e transactions at this place makes it more vulnerable. The persons having their presence online has to see both the business to be carried out at e-media & to save the data or privacy of their customers as well.

ANALYSIS

Over the last few years there has been a noticeable boom in the E-Commerce market. Here the transactions as done over the internet are sensitive to breach of information. The laws prevalent in India and for that matter in the world are not standard to save the online retailers from a breach and customers of the retailers from getting their data stolen. As the time progresses the attackers of the Internet world are also progressing with their methods, the concept of finding a loop in the system is very tempting to these attackers. Whether unencrypted data is at rest with the online retailer or is being used in transactions, the ways to manipulate that data has been sophisticatedly brought into existence by creating certain malwares by these online attackers.

After a well-known retailer has been compromised, it's agile for distinct attackers to put to use the alike tools and techniques to distinct retailers. It doesn't uphold that attacker comprehend where unencrypted payment disclosure might fit within a retailer, whether at glut or transmitted. Attackers have therefore adapted disparate techniques for harvesting disclosure by the agency of increasingly perfected malware.

The unassailable point of intervention in display breaches hasn't been by way of explanation sophisticated anyhow the malware is and attackers are relying on standard position vulnerabilities, misconfigurations, as amply as bomb phishing for their champion entry point. Another as outlook is that attackers have compromised trusted trade partners and trade providers by befriending them, they are targeting in term to win directed toward networks.

Cyber criminals urgently design malware by way of explanation for POS infiltration. BlackPOS is soon available in a proven source format on the blind as a bat web. So at the same time hackers' tools and techniques are escalating, E-Commerce defences are not up.[1]

THE DARK WEB & CYBERSECURITY

Now we shall delve into a dark land of the dark web where security doesn't reach but e-commerce still flourishes. The dark web gives shelter to the underground market places which generally are into the business of dealing with goods and services which are mostly illegal. So when you access the dark web the chances of having your data stolen gets higher and beyond the threshold which a normal online consumer takes into consideration. However, according to a new Global Commission on Internet Governance report, the number is much larger. Just 0.03 percent of the so-called Deep Web is available to search engines, while the even-deeper Dark Web is deliberately hidden and unavailable when using standard browsers.[2]

The Dark Web is "a part of the Deep Web that has been intentionally hidden and is inaccessible through standard Web browsers." Powered by networks such as I2P and Tor, this hidden DarkWeb makes it possible for users to remain entirely anonymous. This anonymity in certain situations might be used simply as a way to protect free speech or for government agencies to keep secret data under curtains, there is another side to this darker corner of the Web filled with cybercrime, the transfer of illegal goods and even terrorism.

Now the question is whether there is cyber security possible to this environment?

In the near future it shall be possible as there are steps being taken in order to deal with this situation but the free movement of the virtually dark place is going to be hampered. The inculcation of cyber security in this kind of illegal E-Commerce shall be done by 6 ways according to the Global Commission on Internet Governance Report which are

Mapping the Hidden Services Directory: Both I2P & TOR use a distributed hash table system to hide database information. Strategically deployed nodes could monitor & map this network.

Customer Data Monitoring: There will be no monitoring of consumers themselves, but rather destination requests to track down top-level rogue domains.

Social Site Monitoring: This includes watching over popular sites such as Cyro, Fmov, Pastebin to find hidden services.

Hidden Service Monitoring: Agencies must "snapshot" new services and sites as they appear for later analysis, since they disappear quickly.

Semantic Analysis: A shared database of hidden site activities and history should be built.

Marketplace Profiling: Sellers, buyers and intermediary agents committing illegal acts should be tracked.

Thus this is how one part of the E-Commerce shall be dealt with in the near future. The focus on the dark web has been made primarily because the dark web has more roots than the standard e-commerce retailers. The concept of Cyber Security contrary to the popular opinion has reached to a very low margin of the internet.

If we analyse the situation we can find that there are innumerable changes to be made in the way Cyber Security is used to protect E-Commerce.

FINDINGS

The findings stumbled upon by delving profoundly in the Cyber Security world we gather that the amount that a virus breaching Cyber Security in 2004 called MyDoom caused an estimated financial damage of $38.5 Billion.[3]

These days the social media has also started earning through the means of e-commerce by selling various games and articles to be used on their web-services online. They also are very vulnerable to be attacked as they are not very well protected by the Social Media provider. Currently, through in depth statistics, there are more than 1.6 billion social network users worldwide mutually more than 64% of World Wide Web users accessing social media services online. Moreover, social networking is one of the virtually popular ways for online users to spend their time, and a preferred way to stay in contact with friends and families. This is precisely why cyber attackers like social media too. Users that spend a lot of time on social networks are indeed likely to be of one mind links posted by trusted friends, which hackers evaluate to their advantage. Here are several of the practically popular types of cyber-attacks started at social media platforms:

Like-jacking: occurs when criminals post shovel Facebook "like" buttons to webpages. Users who get along well the under size don't "like" the gofer, anyhow instead reorganize malware.[4]

Link-jacking: this is a train used to redirect such website's links to another which hackers handle to redirect users from trusted websites to malware infected websites that flee drive-by downloads or distinctive types of infections.[5]

Phishing: the stake to fall in to place sensitive information one as usernames, passwords, and credit ovation details (and regularly, to the side, money) by disguising itself as a good as one word entity in a Facebook front page news or Tweet.[6]

Social spam: is objectionable spam blithe appearing on social networks and barring no one website mutually user-generated easy going (comments, tell tales out of school, etc.). It can fall in to place in multiple forms, including body messages, expletive, insults, hate style, vile links, crooked reviews, crow friends, and by word of mouth identifiable information.[7]

These findings very well establish that there is a need for Cyber Security in E-Commerce and the most important part of it is to spread awareness to the web accessing world. Thus these findings only take us to a stand of disparity amongst people willing to take up an initiative thinking that something might be or is wrong & people willing to overlook the hazards that the world might face when there is a complete developing change in the E-commerce arena.

CONCLUSION

The prime way to avert the risks in the market of E Commerce and building up Cyber Security is to make the consumers of the E Commerce market aware about the situation. There is no secondary alternative to that. Therefore the burden of having the consumer and customer secure shall be on the E Commerce business provider.

From the Ecommerce Side-

E-commerce sites prefer to do as Romans did to their security architecture to equal the demands of ensuring consumer data hideaway and that mix resources are not second hand to attack distinctive Internet sites. A service can certainly survive the commendation generated if their join is hand me down to attack another site. It most definitely wouldn't bear the brunt of if word gets on the wrong track that customer ace up sleeve, buy, or personal data is stolen or copied without their lifestyle or permission. Software developers require to develop the software that is engineered for shelter and security. It is still vacant to add ease-of-use features nonetheless they should be initially turned off. Automated warranty updates are another feature that could be hand me down to help oblige the degree of these attacks.

The application of firewalls at the institution is very valid means to protect data losses. It is also advisable to have segregation of the data at the website. This ensures that the losses can be prevented in certain heads of the storage.

One can also improve the remote access means to avoid the losses, that is to say that Virtual Private Network can be used if remote access is required. A VPN is an encrypted data channel for securely sending and receiving data via public IT infrastructure (such as the Internet). Through a VPN, users are able to remotely access internal resources like files, printers, databases, or websites as if directly connected to the network.

Training for employees could also be a good option as a remedy for the prevention of the losses from lapses in cyber security. Many e-commerce companies are keeping it as an essential part of apprenticeship, but even with help of hackers this training can be given.

The team at the organization should also be able to tackle the incidents of cyber security by formation of team looking for

the cyber security measures. This should be ready well in advance to the incidents or with the probable incidents that may affect companies in toto.

From the Consumers/Customers side-

The consumer on the E-commerce market shall be aware and also should have own protection against such attacks, the valuable insight on how it shall hamper your transactions whatever scale they may be also are important as in the longer run it is important to notice that the attacker can wait longer and steal momentarily over a long period of time. Thus the basic gimmicks of the internet world shall be paid attention to if not understood by the consumer or customer on the E Commerce market.

The customers should keep very strong & inaccessible password to protect hacking or any unwarranted ingress into their details.

This requires a lot of awareness work on the part of the people who are using internet for e-commerce. The training can be given in formal as well as informal means. May be it can be inducted as part of study by students.

Going through a large number of articles and subject monographs by scholars, we have come to a conclusion that there is still a long way to go for our Country as well as globally to comprehend and make aware the subjects of the respective nations about the pros & cons of the E Commerce market access without security. This when done shall result in a more conducive environment virtually.

REFRENCES

1. Cyber Security by Ken Westin, Tripwire
2. The Impact of Dark Web on Internet Governance and Cyber Security Report by The Global Commission on Internet Governance, 2015, Michael Chertoff & Toby Simon
3. The Heimdal Security by Andra Zaharia
4. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013