E-tailing through Social Media - A Cyber Security Threat to Indian E-Commerce



Prof. Rohin Bhatanagar[1] **Dr. Rumna Bhattacharya**[2] **Dr. Ratna Sinha**[3]

Indian E–Commerce is facing cyber security issues since the inception of active contents. Today all consumers are buying and purchasing products online and transacting online through credit cards and debit cards. The product purchase cycle and web engineering are regarded to be the safest by all the online portals but still many loop holes are available with regard to cyber security, server management and protection of consumer database.

Today Social media is playing a vital role through tools like Facebook, Whatsapp, Twitter and many more to follow; all are floating on cloud computing through JAVA scripts and Active X controls. These cloud computing tools are again subjected to cyber distortions through remote substances entering your configurations because of poor server management issues.

This study is all about minimizing the threats as India wants to go Digital, but are we ready in terms of Infrastructural facilities? Cyber threats cannot be eliminated but yes can be protected to major extent to avoid consumer loss and their faith of going digital.

Key Words : *E-commerce, E-Tailing, Cyber Security, online portals.*

INTRODUCTION

What are Cyber threats?

Cyber Threats are commonly found in Active moving web pages or design that are animated, earlier HTML was widely used to design web pages and websites that were static in nature (2005, Sengupta & Majumdar). Today Web designs are multi-momentum activities with the introduction of Apps due smart phones and internet or e-commerce revolution.

These threats are induced through viruses and malwares through unknown encryption that enters your server unit and corrupts and modifies the inputs and coding's provided by the actual users, major malwares are Trojan horse, BugsWorms, file virus, boot sector virus, script virus, ransom ware, SQL(structured query language) injection attack

E-commerce and its revolution story!

E-commerce and its revolution was addressed by globe in the year 2000, India addressed its revolution in the year 2005 and e-tailing gained popularity in 2009 and in India since 2012 with E-commerce revolutionized entire population.

Today all activities of e-commerce are triggered through cloud computing and are imperiled to security reasons. Today E-commerce is a part of active displays and moving graphics through apps and web portal platforms. Though the e-commerce transactions are basically secured through SSL (Secured Sockets Layer) Protocol, and by Public Key Information (PKI).

Server Security

Server security is a challenge to e-commerce portals and websites as the rapid number of increments in cyber security breaches are reported in town every day, privacy & data protection are another concern for e-commercial giants to protect their customer base and data.

Recently ransom was charged by cyber goons through blocking the servers in return to release the data and confidential documents on the cloud. These are due to Poor Server Management in our country and outdated server's (Shipra Srivastava, Oct 2013), which are still in a pathetic sluggish condition that cannot be replaced or upgraded in a day.

Social Media & its implications

In the few decades Social Media have replaced different forms of advertising due to four major factors, Affordability, Accessibility, Availability and Adventuring.

Today Indian Internet and E-commerce are flowing through digital wires through mobility from the technique called cloud computing. The traditional marketing & Advertising techniques do exist, but are cost bearing and less vigorous in nature.

Modern Advertisers are focusing on Social apps such as Whatsapp, Facebook, Twitter, Linked-In, You tube and

[1] Research Scholar, IUJ, IBMR-IBS, Bangalore, rohin3097@gmail.com
[2] Associate Professor, IUJ Ranchi, rumna2006@gmail.com
[3] Professor, ISBR Bangalore, drratnasinha@yahoo.co.in

many more to compel the consumers go online through these mechanisms.

Its implications are compounded in the field of techno-Marketing activities through e-tailing tools such as web portals, shopping apps, e-payment gateways and online marketing designed based applications.

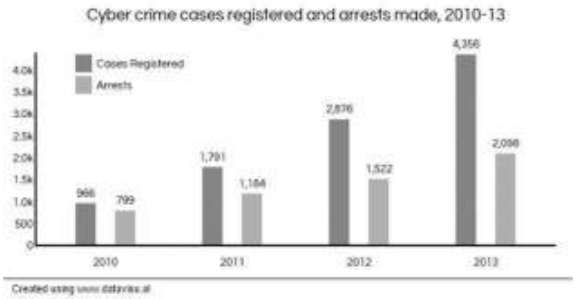
When all such activities are exposed to cloud, security paves its mark and caters caution to these e-players; to secure their e-wires by any threat through the alien body or substance that can infect or de-frame the entire structure of these portals by minute absenteeism of cyber protection. Globally as of today, many measures are taken to protect e-mechanism of these consumer portals from any threat, but shrill hackers are able to device new mechanism to break the fire wall and entire exercise remains futile, despite of firm protection that proves to be fragile in the long run context.

Relation of E-tailing & Cyber threats

E-tailing is a replaced version of earlier "Brick & Mortar" concept of shopping, where consumers used to have footfalls and purchase products through visiting the physical stores. These are replaced by "Click & Monitor" concept where consumers are shopping online through e-commercial websites and portals, the physical walls are altered into shrink eye surveyed optimizers through apparatuses such as Lap tops, Palm tops and ultra-modern invention called Smart Phones.

Today facility of internet is economical and affordable by any section of consumers of Indian markets due to existing tele-communication boom and players, who are catering the demand with analogy of latest slogan in India called "India go Digital". We are not here to thank the inceptors of Digital India, but warn them about lack of Infrastructural fractures that they have and are inviting threat like Cyber hacking, Server breakdown, ransomed calling and many more through alien devices interrupting our technical structure.

A Statistics of Arrests by Overall Cyber Crimes registered in 2010-13



Cyber Threats to E-Commerce Sites

As stated earlier due to cloud computing mechanism cyber threats have increased and are hindering growth of cyber security in India.

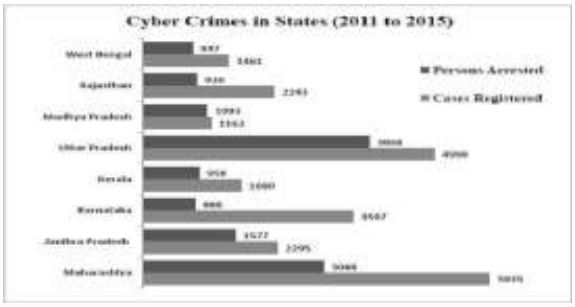
Cyber threats in general to e-commercial sites can be Authenticated, Integrated , Given a Access control, Non repudiated and sourced through Availability; **Authentication**: Authentication establishes proof of identities. It helps in ensuring that the source of an electronic document or message is identified correctly**. Integrity**: The integrity of the message is lost, when the sender sends the message but its contents are modified before reaching the intended recipient, Integrity of message must be intact i.e. message must not be manipulated during transition. **Non repudiation**: It is a situation where the sender denies later on that the message was not sent by him/her. It does not allow the sender of a message to deny the sending of that message **Access control**: Access control determines who has the access of what, because from the security perspective not just everybody can have the access of the system. **Availability**: Availability ensures that the resources are available to authorized persons at all times.

The modern e-tailing is affected by the copiousness of threats; the majorities are Cyber Fraud's, they are namely; *Fraud or Fraudulent in General*, The Identity theft, Friendly fraud&Clean fraud. The modern attacks are by following frauds:

Affiliate fraud : Affiliate fraud is of two types, both of them have the same aim: to pick more money from an affiliate program by manipulating sign up or traffic statistics. This is done either by getting real people to log into merchants' sites using fake accounts or by using a fully automated process. This type of fraud is payment-method-neutral, but widely diffused.

Triangulation fraud : The triangulation fraud is committed via three points. The first is a falsified online shop is used to offer highly demanded goods at very low prices. Many a times, additional bait is added, like if the goods are paid for, using a credit card the information then only goods will be shipped immediately. This fake store, collects credit card information and shipping address–which is the sole purpose. The second point of the fraud triangle is that the fraudster then orders goods at real store by using stolen name and credit card data, and then ships them to the original customer. The third point of the fraud triangle is, the fraudster uses the stolen credit card details to make further purchases.

Recent statistics of Cyber Fraud in India (2011-2015)



Maharashtra in India stood the cybercrime state with 5935 cases that were registered in 2011 till 2015, where the success rate of arrest was 52%, where Mumbai, Pune and Nagpur stood cybercrime estates. It was followed by Uttar Pradesh (U.P) second with 4990 cases registered with 77.5% success rate being, Noida, Lucknow and Ghaziabad are topping the charts. Compared to Maharashtra, success rate was more in Uttar Pradesh arrest. Karnataka- IT state of the country took the third spot having 3597 cases registered against only 888 arrests were possible, which shows the inefficiency of Karnataka police and cyber cell to track cases and give results. This shows how our law and system in the country is active and ready to tackle cyber-attack in India. Bangalore State capitals accounts for third largest E-tailing city after Delhi and Mumbai, Talking about digitalization will not serve the purpose; "Actions speak louder than words" fit well in this context.

Possible solutions to resolve issues in Indian E-tailing

Any day Cyber security is a threat, but resting down your weapons against them is also not advised. In the way of Server security, Portal security and others E-commerce have devised many tools for security nub are; Public Key Infrastructure (PKI), Passwords, Encryption Software, Firewalls: Software and Hardware, Locks and Bars, Digital Certificates, Digital Signatures Biometrics: Retinal scan, fingerprints, Voice etc.

Conclusion

Hereby it is clear that, now a day's internet is widely being used to Buy and sell the items online. With the findings we can conclude that Cyber threats and security are Two faces of the same coin which requires a specialized mechanism where India as a country is still lacking basic infrastructure resources from the Govt. E-commerce to sustain & to protected will require out of the box thinking to the developed software's to tackle file viruses, boot sector virus, Ransomware, which are not only threat to our nation, but are also causing a global threat which both I world nations, II world nation and III world nation have to integrate together to save E commerce in the long run.

References:

- A. Sengupta & C. majundar along with M.S. Barik.E-commerce security-A life cycle approach. Dept of IT Bengal Engg.& sci. university Shipbun-april/june 2005- Sadhana vol. 30 part 2/3.
- Ms. ShipraShivastava Oct 2013.Journal of IT & Computer science,2.
- Charts and statistics(2015) .Govt. of India/cybercrime and security cell.Journal of IT & computer science.
- Charts and statistics (2014).Govt. of India/cybercrime and security cell. Journal of IT & computer science.