Emerging Trends in E-commerce and M-Commerce : Digital Advancements, cyber threats and Law

Dr. Amanpreet Kaur
Assistant Professor, Amritsar Law College, Amritsar, aman_batala15@yahoo.in

ABSTRACT :

The rapid progression in science and technology at an unmatched speed has opened door to e-commerce and m-commerce like never before. The retail markets are touching an impressive $600 million mark. Yet the surprising fact is that e-commerce constitutes barely 5% of the total share in contrast to the 15% in the US. This is clearly an indicative call for sufficient and timely action. What one needs is a SWOT analysis of the situation to study why we have failed to achieve the desired growth levels and how can the lacunae be filled. A deeper insight into the issue reveals that growing cyber crimes and frauds are the chief culprits. Even though the electronic medium is an easy way to buy and sell goods, most of the times, such transactions are wrought with fraudulent means thereby causing a sense of insecurity among buyers. Organizations and companies widely invest in employing the web services to launch new products. When such services are provided, they involve a lot of exchange of information which, if used for illegal purposes can cause serious security threats. The present paper attempts to review the techniques which help in detecting, preventing and predicting cyber crimes in the initial spaces. Ambitious initiatives like Digital India have no doubt increased the user base for internet and given the much needed push to the e-commerce and m-commerce trends; but we need to tread with caution. Inadequate cyber security has damaged the reputation of e-commerce sites and results in significant financial and information losses. The researcher attempts to study this growing nexus between online retailing and cyber theft.

Keywords : - e-commerce cyber m-commerce, theft, digital market, economy retail.

Introduction : - The unprecedented pandemic caused an unexpected upheaval in the global marketing scenario. It was a case of desperate times, that called for desperate measures. The tremendous metamorphosis changed buyer needs and shopping preferences. Shopping habits and lifestyles have changed over the year. A positive indicator for the e-commerce and m-commerce sites is that India's total internet user base has witnessed sharp acceleration from 665 million in 2015 to 829 million in 2021. The potential of e-commerce is immense and the current users touching almost 50 million is first an indication of the under penetration of digital system in marketing. The number actually indulging in active purchasing on a monthly basis is reduced to a meagre 20 million. If this gap is to be bridged and if India wants to create an image of a global e-commerce lynchpin the trends of erratic e-shopping need to be researched and online shopping should be facilitated. It should be a seamless and comfortable experience and there should be minimum disruption. Mobile commerce is even more convenient and accessible. The age of information technology has pervaded every aspect of e-commerce; but it has also given boost to cyber-crime. Fear of cyber crime and theft is a big threat. Cyber laws need to be revamped to prevent further damage to e-commerce and m-commerce. Electronic revolution can be termed as the second major revolution after the industrial revolution. It has inter-connected us globally. India is on a rally of growth but the pace does not match the internet penetration in India. Theft of financial information to business espionage needs to addressed with urgent intervention to boost the marketing scenario in the electronic world.

Challenges and threates to growth of E-commerce and M-commerce : The fear of cyber crime looms large : -

Yougal Joshi and Anand Singh (2013) suggested that "laws will be more flexible to adjust the situation and more and more cybercells to be established to enforce the law". The Parliament realised the seriousness of the issue and to fight the fast spreading cyber-crime, the information technology bill, the IT Act 2000 now, was passed. It provides legal legitimacy to electronic records. Electronic markets are changing faces daily and physical markets are getting obsolete and being replaced by digital screen market space like everything else. This advancement comes with tis share of drawbacks and ailments. Buyers are looted of millions of users of huge money and persoanl data theft which has proved to be the biggest hurdle in online business. Cyber world offers smooth shopping experience with no holidays, no time limits and no bounds of distance. Shopping is at the check of a finger and most banks have set up their desktop and mobile formats to ease online transactions. Global giants like amazon, e-bay, flipkart have devised a new roadmap for shopping. RBI has also given permission to mobile wallets and payment, banks for financial transactions- paytm, vodafone, SBI buddy, ICICI pockets to name a few. While all these may book luring, they also become breeding ground for crime. All the informaton that in shared electronically is on the target of cyber criminals with increase in technical base, we are getting heavily dependent on internet for transactions – but little do we realize the risk associated with it. Financial data is manipulated, electronic ownership is shifted and all this causes a big dent to owner's reputation and even bring a e-business to closure.

The international Fiscal Assocation clearly states "E-commerce refers to commercial transactions, in which an order is placed electronically and goods and services are delivered in tangible or electronic form. If we have a holistic framework in place, e-commerce will definitely see a boom. As we move towards the age of digitization and networking, it undoubtedly ushers in a range of benefits but correspondingly it gives rise to new criminal methodologies. The IT act 2000 and National Cyber Security Policy are too miniscule looking at the gigantic nature of the crime. Cyber Vandalism, cyber violence and even cyber rape are glaring crimes which find no legal status under cyber crime. So, be it e-commerce or any other aspect of electronic work, law definitely lacks enforcement.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

Cyber crime in which the computer is a target or tool or both is definitely an unlawful act. India is smartly marching to be the new e-frontier where a rapidly expanding citizen base with smartphones are looking at breaking the scenario of physical shopping.

Internet connection in India (in millions)

	2014	2015	2016	2017	2018	2019
Wireline (in millions)	20	22	25	27	30	32
Wireless (in millions)	210	273	337	402	469	528

Source : KPMG India Analysis

This is just the rosy picture; the dismal side is that still a wide population is not computer savvy and breach of security and cyber theft are potent threats. Fraud, forgery, defamation and mischief, through electronic media all find a place of crime and IT act 2000 which was amended in 2008 to widen the purview. The cyber crime gets even more complex with unsecured networks, IT infrastructure, lack of awareness in consumers. Cyber crimes in India are registered under two different acts- The IT Act and the Indian Penal Code. Tempering with computer source documents (65 IT Act), Hacking (Section 66(2) IT Act) publishing false digital signature (Section 73 IT Act) are some crimes in cyber world that have found serious punishment under the IT Act. Similarly, cases registered under the IPC include false electronic evidence (section 193 IPC) destruction of electronic evidence (section 204, 477 IPC) etc. Computer is a big weapon in computer generated cyber terrorism, credit / debit card fraud, EFT frauds, virus attacks and the like.

Harpreet Singh Dalla and Ms. Geeta (2013) concluded that “the use of internet are increasing in the world in a large number rapidly, here it is very convenient to gather any information within a moment by using internet as huge source of information. . The concept of e-commerce started in the 1970’s. The concept carried with it the threat of cyber crime and the resultant rules which gives legal recognition for transactions carried out by means of electronic data interchange. The council of Europe’s cyber crime treaty uses the term “cybercrime” to refer to offences ranging from criminal activity against data to content and copyright infringement. Thus cyber laws aim to provide safety from online fraud, humiliation, unsocial content on internet and illegal human activity on the internet. Large customer base, law awareness, comparatively less strict rules have made India a soft target for cyber criminals.

Total number of cases registered under cyber crime

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
	1322	2213	3477	5693	9622	11592	12317	21796	27248	44546	50035

Sourced from NCRB

As the business activities evolve in the umbrella of the cyber world, internet is like a candy for the cyber criminals. Strong laws, awareness in people and use of technology are essential to prevent activities that are a threat to cyber security. We must also remember that in India e-retailing is in its initial stage and even though more and more buyers are joining the voyage. The laws related to cyber crime are far from effective. The first time buyers are specially easy prey of cyber attackers.

Also, since fewer buyers are comfortable with online banking, COD i.e. cash on delivery is a more viable option. Physical payment collection gives easy ground for criminal activities – wrong delivery addresses are provided which causes huge loss to the e-retailers, specially in COD option. Data theft has been another worrisome issue-Ashley Madison where the "Ashley Dating website" was hacked. Hackers claim to hack data of over 37 million users including their card numbers (Desk, 2015) though this may not directly impact e-commerce but data leak through credit card details shared on e-commerce sites can actually lead you to a quagmire of other crimes. Bank security systems are also not spared "Kotak Mahindra Bank in 2015 reports fraud of Rs.2.82 cores in 1730 transactions in 7 countries with the 580 cards which have never been issued – All cards were fabricated using BIN (Bank information number (Narayan, 2015)

One of the major shortcomings of the IT Act 2000 is that territorial jurisdiction is the major issues which is not satisfactorily addressed. On most occasions, the investigator refuses to take complaints on the issue of jurisdiction. IT Act definitely needs revision and there should be provision for scientific, technical and professional training for lawyers in India to handle such issues. Cyber Crime is easy to commit but hard to detect given the geographic indeterminacy of the net. This is ironic if we see the statistics provided in the report published in the times of India on 6th September, 2015 which states, "The Indian E-Commerce Industry grew by 33% in 2015 clocking sales of Rs. 62,967 compared to Rs. 47,349 in 2012." The corresponding growth in cyber crime bring to the forefront that it is indeed a struggle with the internet to find a way to safety buy and sell goods or to transfer funds using computer and telecommunication networks. E-commerce and M-commerce offer huge business opportunities to small industries find a market for their products. Most small retailers try to host their business on the web and penetrate under market base through suitable advertising campaigns since there is no involvement of high rentals and no boundation of time and distance the retailers see greater chances of profit. The exponential growth of e-commerce is a result of internet driven initiative. Preventing cyber crime requires a strong e-security rather than more human prudence. The role and efficacy of cyber laws have been in question as technological invasions limit individual privacy. The cyber crime may pervade all forms of transaction – business to business, business to consumer, consumer to consumer or consumer to business. A variety of applications are put to use in e-commerce-emails, online catalogues, shopping carts, EDI, File Transfer, Protocol Web Services etc companies try to entice the consumers directly online using tools such as digital coupons and targeted advertisements.

Just as wolf's eyes prey hen's pen, a hackers eyes are always scurrying to steal your data stored online. Their constant endeavour is to rip off your personal credentials provided during your transactions from online databases. What you need to get clearly is that internet is definitely not a safe place to hoard your personal data. The entire e-commerce business is pillared on trust. To quote Jack Ma, the founder of Alibaba" For E-commerce the most important thing is trust." This is the absolute truth given the fact that the biggest of business are bound to crumble if customers lose faith and trust. It is very important that customers be trained to know how they can keep their information safe, what counter active measures to adopt, what are the common mistakes customers can steer clear off on the part of businesses, the least they can ensure is that they have a host provider who can store up and running without downtime interferences. It is always advisable to opt for quality and reliability over cost affordability. To every customer indulging in e-commerce, the key rule should be to have the minimum sensitive information shared online – the less you store lesser are the chances of major losses. Never store user names, pin codes and other critical information on online portals. Rather keep them stored offline that can only be accessed by you when the need arises. In some cases cyber cheaters are the retailers themselves. "The retailers of electronic shopping websites are shipping the wrong/false products to the customers, as the payment is done before the delivery of product and customer cannot predict that seller is genuine or not HUL has confirmed the fake products.

(Lakme Eyeliner Eye conic) sale on e-commerce giant FlipKart by various sellers." Jhulka, 2015) Cyber frauds like these are also cybercrimes because they use the online methods to trap the customers. At times, even the sellers indulge in criminal activities. It has been reported that vendors make order themselves and then replace the order on arrival and complain against the faulty products." E-commerce companies are committed to collect the returned product which is actually changed by fake buyers and return their money." (Shenoy, 2015) Such cases have been reported by both Amazon and FlipKart. To control such situations there has to be mutual co-operation between business houses and buyers. .

Conclusion The focus of the paper centers around the penetration of cybercrime into the marketing area in India and its impact across different levels of society. The findings and research are clearly indicative that in the Indian prospect as the business in e-commerce is increasing, the trend and pace of cyber crimes is also gaining momentum. This has worked as a great deterrent to growth and development of e-commerce and m-commerce. The need of the hour is stricter cyber law enforcement agencies and utmost security measures for data protection. The business indulging in online trade must ensure that the software's they use do not fall easy prey to hackers because if the sensitive information shared by consumers for purchase of goods is misused it leads to breach of trust which can cause serious damage to the organization-both in terms of financial loss and damage to the reputation. E-commerce requires careful planning and co-ordination of a number of technological infrastructure components which can trace and prevent cyber attacks. We must collaborate globally to develop an effective model that can fight against such fast spreading cyber crime on the part of the consumer, one needs to beware And not share personal information like user id, password etc. Try to keep yourself protected by installing basic security programmes. Never get lured by emails promising Lottries, prizes and gifts. Always ensure to login with a secure connection and last but not the least always set passwords that are difficult to predict. If one takes sufficient caution and if the law enforcement gets stricter e-commerce is bound to be on the road to success and cyber crime will be a thing of the past.

References

Dalla, Er. Harpreet Singh., & Geeta, Ms. (2013). Cyber crime- A threat to persons, property, Government and societies. International Journal of Advanced Research in computer science and software Engineering (IJARCSSE), 3(5), 997-1002. Retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V315-00374.pdf.

Joshi, Youghal, & Singh, Anand. (2013). A study on cyber crime and security scenario in India. International Journal of Engineering and Management Research (IJEMR), 3(3), 13-18. Retrieved from http://www.ijemr.net/DOC/AStudyOnCyberCrimeAndSecurityScenarioInINDIA(13-18)48f66c6f-4d11-4f64-95ec-a3600f6cd9d3.pdf.

Kaur, Rupinder Pal. (2013). Statistics of cyber crime in India: An overview.International Journal of Engineering and computer science (IJECS), 2(8),2555-2559. Retrieved from http://www.ijecs.in/issue/y2-i8/41%20ijecs.pdf.

National Crime Records Bureau. (2016). Crime in India 2015: Statistics, New Delhi: Ministry of Home Affairs, Government of India. Retrieved from http://ncrb.nic.in/:http:ncrb.gov.in/.

Arpana, & Chauhan, M. (2012). Preventing cyber crime : A study regarding awareness of cyber crime in Tricity. 2(1).

Dest, T. (2015, Aug 19). Ashley Madison Hacked : Here’s Why the website for ‘cheating spouses’ got targeted. Retrieved Jan 10, 2016, from http://indianexpress.com/: http://indianexpress.com/article/technology/social/ashley-madison-data-breach-why-the-website-for-cheating-spouses-got-backed/

Dhanao, R. (n.d.). Cyber Crime Awareness. International Journal in Multidisciplinary and Academic Research (SSUMAR), 2(2), 1-7.

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/2015-11-20/news/68440486_1_flipkart-satinder-singh-drivers.

Kandpal, V., & Singh, R. (2013). Latest Face of cybercrime and its prevention in India. International journal of basic and applied sciences, 2(4), 150-156.

(2015), Law & Technology: Evolving challenging as a result of fraud in E-commerce sector. 5 Grant Thornton India LLP.

Mehta, S. & S Singh, V. (2013, Jan). A Study of awareness about cyberlaws in the Indian Society, International journal of computing and business research (UCBR). 4(1)

Maneeesh Taneja and Dr. D.B. Tiwari, "Cyber Law", International Referred Research Journal, Vol. 11 (21) October, 2010, pp.63-65.

Patel, Ravikumar S., & Kathiriya, Dhaval. (2013). Evolution of cybercrimes in India. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2(4), 240-243. Retrieved from http://www.ijettcs.org/Volume2Issue4/IJETTCS-2013-08-15-086.pdf.

Saini, Hemraj., Rao, Yerra Shankar., & Panda, T.C. (2012). Cyber-crimes and their impacts : A review. International Journal of Engineering Research and Applications (IJERA), 2(2), 202-209. Retrieved from http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf.

United Nations Office on Drugs and Crime (UNODC). (2013, February). Comprehensive study on cybercrime : Draft. New York, Vienna : United Nations.

http://cse.standor.edu/class/cs201/projects/computer-crime/theft.html.

http://legal.practitioner.com/computer-crime/computercrime_3_2_7.html.

Lech.J. Janczewski, Andrew Colarik, Managerial Guide for Handling Cyber-terrorism and Information Welfare, IGI publishing, Hershey, PA, 2005.

Carr, I., 'Anonymity, the internet and criminal law issues', in C. Nicoll, J.E. J. Prins, J.M. C Asser Press, pp. 197-206 (2003).

Sankar Sen 'Human Right & law enforcement'. 1st ed., Concept publishing New Delhi (2002).

Dr. Subhash Chandra Gupta, 'Information technology Act, and its Drawbacks', National Conference on Cyber laws & legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad (2000).

Dr. Farooq Ahmed, 'Cyber law in India (laws on internet)', Pioneer Books, Delhi U.S. App (1992).
s://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/18-Cyber%20Crimes_2012.pdf

https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html

https://factly.in/data-the-number-of-registered-cyber-crimes-cross-50000-in-2020-20-of-these-are-fraud-cases/