Review Article

Study of Online Cyber Crimes in India

Subhash Desai*

SAL Institute of Technology and Engineering Research, Opp: Science City, Sola Road, Village – Bhadaj, Ahmedabad – 380 060

Address for Correspondence

SAL Institute of Technology and Engineering Research Opp: Science City, Sola Road, Village – Bhadaj, Ahmedabad – 380 060

E-mail: subhash1948@yahoo.com

ABSTRACT

Cyber crimes are a new class of crimes to India rapidly expanding due to extensive use of Internet. Dishonest and greedy people take advantage of easy and free access to Internet and perform any acts to satisfy their needs. The need could be physiological or psychological in nature.[2]

Online shopping and wide use of "social media" are root cause of cyber crimes. Much awareness created for cyber crimes and users were educated. But still people do not complain it to authorities. Even somebody do it then also police or crime branch unable to clear such complains in reasonable time period. Delay in justice will lead to NO registration of complain. This is not healthy situation in free democratic INDIA.

The law IT (Information Technology) Act 2000 and several sections of the IPC are in place but in large population country like China and India, it is very difficult to control crime caused by cyber world. We need to have self control for better society.

We shall evaluate impact of social media, trends towards shopping online and punishment for cyber attackers in this paper. We shall also try to prepare road map for Indian and recommend approach suitable for young generation of India.

Keywords: Cyber Crimes, IPC, Online shopping, Punishment.

INTRODUCTION

We find many products on TV and Internet promoted by popular celebrities as its brand ambassador. There are many hoardings at every street corner and advertisement for products. The name of products is constantly hammering every one's mind. Think, what may happen if product is not seen in market. It is also true for service segments. Despite of making product demand again and again, when product is not reaching the customer, people will drop their demand and may forget products. Same thing is happening with cyber crimes in India.

India is second largest market in world for smart phone. India is at second place regarding face book users and thirty million twitter users. Whatsapp users are around one million. It is expected that in next one year, mobile internet users will be three hundred twenty million and total internet users shall be

five hundred million.[5] We have large network of users but we just have only twenty three cyber crime cell. As per government National Crime Bureau report, there were 9,600 cases reported in year 2014. Unofficial sources indicate that it is beyond 3 lacs.[5]

It is unfortunate that government policy to use cyber crime cell to assist police to solve criminal cases. Thus it often kills basic purpose of this cell. Let us assume that average staff in a cell is 50 then there are 1000 – 1100 people in entire India. Because of internet users are many and limited people in cyber cell, we find that there are lacs of online cyber criminals which are out of control.

"Teenagers groups are becoming victims of collectivism very easily. Collectivism is the tendency of people to emphasize their belonging to groups. The sense of belonging and "WE" versus "I" in relationships is fundamental in this age group. In China, individual rights are a foreign concept to traditional Chinese. Unity is essential when they are confronted with many hardships. For effective control on fraud and crime, we should have Chinese approach. Order is the highest social ideal in china. Buddhism suppresses individual identity".[2]

E-SHOPPING[1]

E-shopping or online shopping or e-store are all virtual types of stores which allow customers to buy products or services over the internet. The best and the most popular online retailing stores are: Amazon.com, eBay, Gmarket, Alibaba. With the growth of online shopping, comes a wealth of new market footprint coverage opportunities for stores that can appropriately cater to offshore market demands and service requirements.

Advantages and disadvantages: Online shopping facilitates customers by providing home services much cheaper and providing more options to choose from. Thus, it is convenient for the people to shop online without spending their valuable time in markets.

There is risk in ordering things online as you cannot guarantee the material, but online shopping systems have good return policies also. But the greatest concern here is of privacy and security.

It is obvious that like any new technology, the IoT (Internet of Things) has the potential to drastically improve our personal lives, work place and industrial capabilities as it is affecting our life directly. End user acceptance is necessary for any new technology.

By the trends and the history of user acceptance, the expectation is that it may take time for users to adapt to new technologies and opportunities of the IoT, just as mobiles and e-commerce have taken years.

Desai Subhash said "Once IoT establishes its ground, we can imagine a totally new environment in our future; it will be user friendly and more users independently". One can imagine what ads companies will do with IoT, how everything will be flourished.

Data exchange is critical in networked world. We are facing the cybercrime challenges and now if we are expecting to have a huge interconnected world of devices, we have to look at our security systems requirement.

Our emails can be hacked so being "connected to the internet" always would mean the possibility of more surveillance, both good and bad. It also means the possibility for more fraud, scams and cyber-attacks.

To ensure that the personal data collected is used only be the authorized service, solutions have already been proposed that is usually based on 'privacy broker'.

But important requirements in IoT is that of security. Here, the person's card information or account information are potential and attractive targets of hacking.

Misuse of e-mail and Personal Information

Information about user's activity on the Web is being recorded and there will be privacy losses. Many users are not aware about it. Web users leave a "data shadow" with information about what they read, where they shop, what they buy, whom they correspond with and so on.

High-volume server can track significant information about a user's browsing habits. Many advertising companies share user profiles and build massive databases containing users and their data shadows.

When users select set of trusted re mailers, the message recipient can not tell where the message originated. There are many such re mailers available for use. Attackers can send junk mail free of charge. If they have to pay for each thing they sent, there would be fewer attacks. It would be harder to steal people's accounts if it cost the victims money. There are ways to keep data safe. A. D. Rubin, D. Geer and M. J. Ranum discuss about security in more detail in their Book **"Web Security Source".**[4]

PUNISHMENT

It is an unpleasant event that follows a behavior and decreases its frequency. However, the use of punishment will have negative effects over long periods of time. It may cause undesirable emotional reactions. It leads only to short-term hide of the undesirable behavior rather than to its elimination.

Educating, guiding and counseling may help in this direction and contribute effectively in minimizing crimes and frauds. We need to apply love force as against any legal or pressure techniques. We need to bring "change" in people who are already involved in such bad manners and habits using following Systems Model of Change.

It is not the strongest who survives nor the most intelligent, but the one who most responsive to change.[2] Hellriegel, Slocum and Woodman discuss this issue in their Book "Organizational Behavior".[3]

Social media is sweet gift from western countries. Even country like USA is not able to control cyber crimes. Hence, they have started taking strict security steps. Outcome of these steps will be known only in future. The basic question is about attitude to control any kind of crimes. India could have adopted western model in this regard. But we miss that opportunity.

CONCLUSION

It is not sufficient. We also need latest technology and more importantly technical staff who understand and make use of this technology. Misuse of social media can be done within minutes, whereas cells are working at very slow speed. It may lead to decades to resolve the cases and by that time in some sensitive cases damage is already done. Time is now to act instead react.

Sometimes there is dependency on foreign agencies. We know that laws are different in different countries. This causes further delay. There is urgent need of ethical hackers who can go to the root cause of criminals. Looking at the growth of social media in India, we require at least Fifty thousand ethical hackers. Good opportunity for such job seekers.

Some of the recent bollywood movies and TV serials broadcast criminal cases and the process of catching the criminals. But in large populated country like India, criminals are becoming smarter and get lesson from the episodes. We as member of society person should consider, think and give right directions to new generations to come.

REFERENCES

1. Desai Subhash, "Understanding IoT Management for Smart Refrigerator", *International Journal for Scientific Research*

and Development (IJSRD), January – 2016. ISSN (Online): 2321 – 0163, Impact Factor: 2.39.
2. Desai Subhash, "Fun and Fraud by Teenagers in Cyber World", Fifth PIMR National IT Conference, Indore, India, September 2010, Pages 336 to 339. **ISBN: 978-81-7446-884-0.**
3. Hellriegel, Slocum and Woodman Organizational Behavior – Ninth Edition Book
4. A. D. Rubin, D. Geer and M. J. Ranum Web Security Source book, John Wiley & Sons, New York, 1997
5. Gujarat Samachar daily News Paper dated 07/02/2016
6. www.seasonsindia.com
7. Yonghui Zhang. "Intelligent Monitoring System on Refrigerator Trucks Based on the Internet of Things", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012, pp. 201–206
8. AviItzkovitch, "The Internet of Things and the Mythical Smart Fridge". ARTICLE NO. 1089 SEPTEMBER 18, 2013
9. eXistdb, http://exist-db.org/
10. Dave Bonouvrie, "Nine Real-Life Scenarios That Show How The Internet Of Things Could Transform Our Lives" http://www.businessinsider.com.au/
11. G.V. Lioudakis , "A proxy for privacy: the discreet box", in: EUROCON 2007, Warsaw, Poland, September 2007
12. Internet of Things http://whatis.techtarget.com/definition/Internet-of- Things
13. Dieter Uckelmann, Mark Harrison, "Architecting the Internet of Things". 1st ed. Springer Science & Business Media 2011, pg 276
14. Electronic Commerce http://en.wikipedia.org/wiki/Online_shopping.

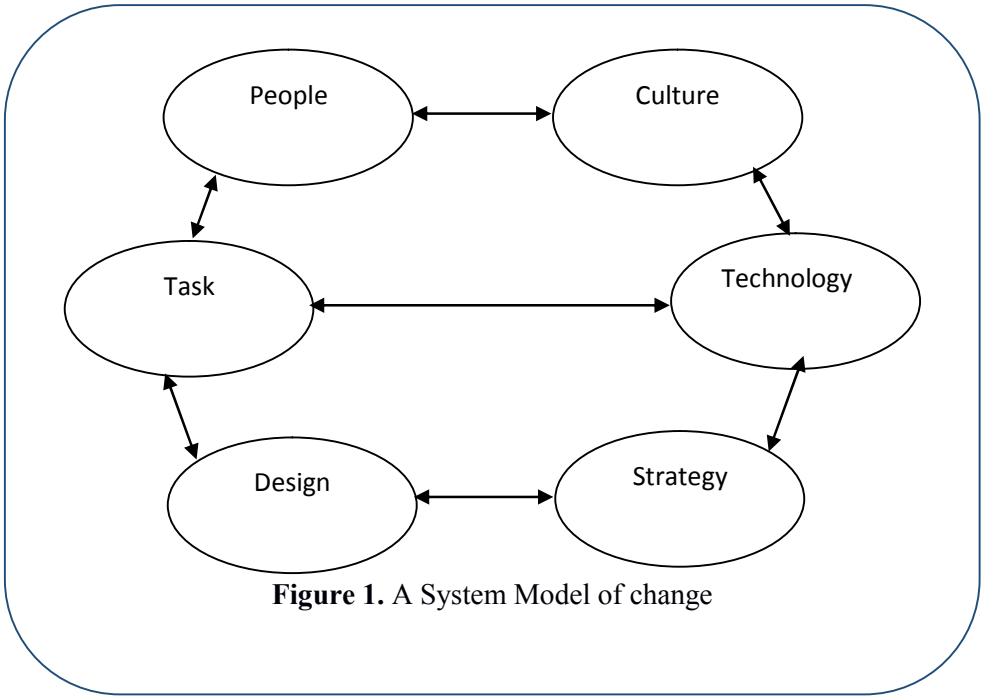

Figure 1. A System Model of change