INTERNATIONAL JOURNAL OF RESEARCHES IN SOCIAL SCIENCES AND INFORMATION STUDIES
© VISHWASHANTI MULTIPURPOSE SOCIETY (Global Peace Multipurpose Society) R. No. MH-659/13(N)
www.vmsindia.org

ECONOMICAL AND SOCIAL IMPACT OF CYBER CRIME

P. V. Meshram
Chintamani College of Commerce, Pombhurna, Dist-Chandrapur.
drpurnimavilas@gmail.com

Abstract
Cyber criminals take full advantages of the anonymity, secrecy and inter connectedness provide by internet, therefore attacking the very foundations of our modern information society. In current era of online processing, maximum of the information is online and prone to cyber threats. There are huge numbers of cyber threats and their behavior is difficult early understanding hence difficult to restrict in early phases of the cyber attacks.
Cyber attack may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as a cyber crime and they have serious impact over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society.
Keywords:- Cyber attacks, cyber crime, consumer trust, threat, economic impact, social impact.

Introduction:

Computer- related crime dates to the origin of computing, though the great connectivity between computers through the internet has brought the concept of cyber crime into the public consciousness of our information society. Improvement in performance is only possible with the use of internet. The term internet can be defined as the collection of millions of computer that provide a network of electronic connections between the computers. There are millions of computer connected to the internet. Everyone appreciates the use of internet but there is another side of the coin that is cyber crime by the use of internet.

In 1995, when the world wide web was in its early stage of development, futurist Dr. Gene Stephens wrote about the present and future reality of cyber crime and made several predication; "Billions of dollars in losses have already been discovered. Billion more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty first century-the cyberspace offender". (Stephens 1995, p 24)

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crime involving computers. Cyber crime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cyber crimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc. In tenth United Nations congress on "prevention of crime and treatment of offenders" which is devoted to issues of crimes related to computer networks, cyber crime was broken into two categories and defined as:

a. Cyber crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by mean of computer system or network.

The Scope of cyber

Law enforcement officials have struggle to identify, arrest, and prosecute these tech savvy offenders, even as sociologists have sought to get to the root of cyber crime .The Federal Bureau of Investigation (FBI) created a special cyber division in 2002 to "address cyber crime in a coordination and cohesive manner (Federal Bureau of Investigation, 2013) with cyber squad in each of its fifty-six field offices," cyber action teams" that travel worldwide to address cyber attacks, and nationwide computer task forces. The field of cyber crime has spawned the field of cyber criminology, defined as "the study of causation of crimes that occur in cyberspace and its impact in the physical space"

The scope of cyber crime remains staggering and it continues to grow. In 2012, for instance, the US economy lost $525.5 million to cyber crime (Federal Bureau of Investigation, 2013) up over 40 million from 2011 with the most common complaints in 2012 begin impersonation email scams, intimidation

crimes, and scams that attempted to export money from computer users. In 2012, cyber crime cost British businesses 21 billion (Morris, 2012), and over one million computer users in the European Union were affected every day by cyber crime (Eeu Active, 2012).

As more and more people have used the internet to do their shopping, communicating, banking, and bill paying, they have become targets for cyber criminals. There are common sense steps that can prevent or reduce having one's financials information stolen online, as well as to avoid other scams and threats, but cyber crime in these areas persists largely due to a lack of consumer education.

Some varieties of cyber crime, such as hacktivism, are ostensibly motivated by noble intention, such as protest against perceived abuses by government and corporation. Often these attacks involve posting comments of official government websites and are not motivated by a desire for monetary gain. However, other forms of cyber crime have a much more violent intent. These include cyberstalk, cyberbullying, and cyberterrorism.

Economic Impact of Cyber Crime

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online.

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies 'surveyed acknowledged financial losses due to computer breaches'. The approximate number impacted was $450 million. Almost 10% reported financial fraud. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.

Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization.

In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more detail.

Social Impact of Cyber Crime

While the economic impact of cyber crime is beyond dispute, rather less attention has been given to the social implications of cyber crime. Psychologists and psychiatrists can help victims cope with the fallout from identity theft, sexual abuse, or financial ruin, whereas sociologists are well positioned to look at the broader social impact and explanation of cyber crime.

Cyber crime attacks the very foundation of modern, technological societies, bound up as they are with rapid flow of computer data facilitated by the internet. At the most basic level, cyber criminals often take advantage of technologically unsophisticated individuals who nonetheless find themselves in a world where the internet plays an increasingly central role in both community and private life. Cyber crime depends, at this level, on the ability of those who are more technologically sophisticated to use that knowledge to trick others into surrending vital information, such as their bank account information or social security number. While it is possible in some situation for the victim of cyber crime to restore stolen money or even their personal online identity, the event often leaves the victim traumatized and deeply

suspicious of the internet and other trapping of modern life.

Conclusion

As someone rightly said that "bytes are placing bullets in the crime world." The growth of cyber crime in India as all over the world is on the rise and to curb its scope and complexity is the pertinent need today. This manuscript put its eye not only on the understanding of the cyber crime. But also explain the impact over different levels of the society. This will help to the community to secure all the online information critical organization which is not safe due to such cyber crimes. The understanding of the behavior of cyber criminal and impact of cyber crimes on society will help to find out the sufficient means to overcome the situation.

India's profile and wealth have risen enormously in the world due to the constructive use of information technology. At the same time, India rank fifth in the world for cyber crime according to a report last year by the US based. Internet crime complaint centre, a partnership between the Federal Bureau of Investigation and the National white collar crime centre.

To sum up, India needs a good combination of laws and technology, in harmony with the law of other countries and keeping in mind common security standers. In the era of e-governance and e-commerce a lack of common security standards can create havoc for global tread as well as military matter.

Reference :-

1. **Bowen, Mace (2009),** Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.

2. **Leagal Info (2009),** Crime Overview Aiding And Abetting Or Accessory, Available at: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, Visited: 28/01/2012

3. **Cyber Crime(2003)** by R.K. Suri and T.N. Chhabra, Pentagon Press,New Delhi.

4. **India Crime in India: 2011-Compendium (2012),** National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
5. http://www.internetworldstats.com/stats.htm
6. http://en.wikipedia.org/wiki/Computer_crime