IJERSS | Volume 12| Issue 2 | FEB 2015

Research Paper

# CYBER CRIME AND CYBER SECURITY

INFORMATION SECURITY

**Keywords:**

| Nirmal Kaur | Punjabi University Campus, Maur Mandi(Bathinda), Punjab |
|---|---|

**ABSTRACT**

Cyber crime is a term used for fraudulent activities done using the channel of computers, the Internet, cyber world and the websites. It is an illegal act wherein computer is being used either as a weapon or as a target or both. Cyber crime can involve criminal activity like theft, fraud, deformation and mischief. The misuse of computer has given birth to new level crimes that are introduced by the Information Act, 2000.A rise in online population has given a path for cyber criminals, with a great losses due to cyber crime in billions of dollars.

## I. INTRODUCTION

The Significant success of internet has become possible because of its relative openness and minimum security constraints to entry for those who operate it with vicious intentions. Cyber crimes are rising speedily with incurring more cost and taking longer to resolve. The 2014 global study of U.S.-based companies, which spanned seven countries, revealed that over the course of a year the average cost of cyber crime jumped by more than 9% to $12.7 million for companies in the United States, up from 11.6 million in the 2013 study. Cyber crime has produced serious problems for employment to developed countries. The effect of cyber crime is to shift employment away from jobs that create the most value. Indian has still not formulated strong cyber law to overcome this increasing graph of cyber crime activity. cyber law is still ineffective in delivering crime convictions, even as cyber fraud continues to increase. The year 2013 has been regarded as how cyber legal threats are increasingly become relevant.

## II .TYPES OF CYBER ATTACK

**Hacking:** Hacking in simple term means an illegal intrusion into a computer system or network. Hacking entails cracking systems and gaining unauthorized access to the data stored in them. Government websites are the hot target of the hacker due to the press coverage.

**Cyber Sqatting:** Cyber sqatting is a act for registering a famous Domain Name and then selling it for a fortune. This is an issue that has not been tackled in Information Technology Act, 2000.

**Viruses and worms :** Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.

**Spam emails:** Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver — potentially creating a wide range of problems if they are not filtered appropriately.

**Trojan :** A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk.8

**Computer Vandalism:** Damaging or destroying data rather than stealing or misuseing them is called cyber vandalism. These are programs that attach themselves to a file than circulate.

**Denial-of-service (DoS) :** DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.

**Malware :** Malware is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a 'botnet'— a network of computers controlled remotely by hackers, known as 'herders,' — to spread spam or viruses.

**Scareware :** Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses.9

Vishing: This term is combination of "Voice" and Phishing. Vishing is a criminal act of using social engineering and voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward.

**Phishing :** Phishing attacks are designed to steal a person's login and password. For instance, the phisher then has access to the customer's online bank account and to the funds contained in that account.

**Fiscal fraud :** By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits.10

**State cyber attacks :** Experts believe that some government agencies may also be using cyber attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an

invisible attack on Iran's secret nuclear program. The virus was aimed at disabling Iran's uranium enrichment centrifuges.11

**Carders :** Stealing bank or credit card details is another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops.

**Cyber Stalking :** Cyber stalking is used to stalk someone by use of internet or electronic means. This term is interchangeable with harassment and online abuse.

## III .CYBER SECURITY

Cyber security, also referred to as information technology security. Its main motive is to protect computers, networks, programs and data from cyber attacks like unintended or unauthorized access, change or destruction etc. According to wikipedia Cyber Security is the process of applying security measures to ensure confidentiality, integrity, and availability of data. Cybersecurity assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. As the number of mobile users, digital applications and data networks increase, so do the opportunities increases for hackers to make bad influence or exploiate the users by using cyber attack. Security alerts and Vulnerabilities greatly impacting their ICT infrastructure . It helps in tracking botnet, phishing sites, spam, malware, etc. and the steps to overcome these issues .Early-watch-and-warning system will protect our machines from cyber attacks . Incident response mechanism also helps in reacting for any fraudulent activity according to the situation. Government's cyber security arm Computer Emergency Response Team-India (CERT-In) reported 62,189 cyber security incidents in the first five months of the current calendar year. During the years 2011, 2012, 2013 and 2014 (till May), a total number of 21,699, 27,605, 28,481 and 9,174 Indian websites were hacked by various hacker groups spread across worldwide. In addition, during these years, a total number of 13,301, 22,060, 71,780 and 62,189 security incidents, respectively, were reported to the CERT-In. The government should give consideration to adoption of security standards and practices which permote basic security that provide immediate response to threats, fluctuations and actual cyber attack with compliance as an outcome. A Cyber Coordination Centre should be set up at the operational level, managed by personnel from the integrate operational agencies. This centre would work as a filtering-house, assessing information arriving in real time and assigning responsibilities to the agencies concerned, as and when required

## IV .INDIAN CYBER LAWS FOR CYBER SECURITY

Cyber security is a critical issue. There isn't really a fixed definition for cyber crime. The growth in IT and developments and quick ease with the use of applications has looked into the use of cyber space. The use of cyberspace growing dramatically. As India progresses, its reliance on the Internet will increase at a rapid pace. As per the cyber crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cyber crime cases were registered under Information Technology Act during the year 2011, 2012 and 2013, respectively, thereby showing an increasing trend. Among the many institutions that came up and have endured are the Internet Engineering Task Force (IETF), set up in 1986. It is a institute with a number of experts on various aspects of the Internet who worked through a cooperative consensus-based decision-making process. One more similar institute was set up in 1998 as The Internet Corporation for Assigned Names and Numbers (ICANN) on similar theories to control the Domain Name System (DNS). Most of the ICANN's powers and functions were devolved to it by the US government, which hitherto controlled DNS. The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

***LAW & PUNISHMENT***

The IT Act of 2008 covers all actions in this domain. Sections 69, 69A and 69B contain provisions for intercepting, monitoring or blocking traffic where, amongst other reasons, there is a threat to national security. Section 70A covers protection of critical infrastructure. There is a need to work within these provisions. Under Information Technology (Amendment) Act, 2008, Section 66-C and Section 419 of Indian Penal Code, 1860 also applicable. Identity Theft offence is cognizable, bail able, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

The IT Act defines the role and legal responsibility of the network service providers in India. Section 79 restricts the liability of service providers in certain cases. Their liability in India is also determined by License for Internet Services, Clause 33 and Clause 34 of which set out the various responsibilities of the service providers, some of which are:

- ISPs must prevent unlawful content, messages or communications including objectionable, obscene, unauthorized content from being carried on their NW (Network).
- They must ensure that content carried by them does not infringe cyber laws.
- They must comply with the IT Act provisions and must assist the government in countering espionage, subversive acts, sabotage or any other unlawful activity.
- Privacy of communication online is ensured by preventing unauthorized interception of messages. Government can take over their equipment and NWs in times of emergency, war, etc.

## V .THE KEY ISSUES FOR CONSIDERATION FOR A POSSIBLE CYBERSPACE CONVENTION

National critical infrastructures should not be harmed. Secure, stable and reliable functioning of the Internet should be ensured. A common understanding of Internet security

issues should be evolved. National governments should have the sovereign right to make national policies on ICT consistent with international norms. A global culture of cyber security based on trust and security should be encouraged. The digital divide should be overcome. International cooperation should be strengthened. PPP should be encouraged. CIA of information systems should be ensured. Balance between the need to maintain law and order and fundamental human rights should be maintained.

**VI .PREVENTION**

Today education & training is most important to understand common hacking problems, such as phising, social engineering etc. Awareness about different cyber attack go a long way to protect yourself against many types of cyber crime. In the digital world, computerization goes on hike. We need better antivirus software to detect, remove, and protect our machines and network from cyber threats. By using antivirus we can secure computers, digital assets and networking.

**CONCLUSION**

Cyber crimes infect the world because we can't restrict the influence of cyber crime so easily. Cyber crime and its hackers will continue developing and upgrading to stay ahead of the law. Cyber security is a safer way to help us against cyber attacks. Many countries like US, Russia, China, and Australia etc. are seriously engaged in improvement of their security doctrines and strategies. The international community is also engaged in a variety of discussions to provide a safe and secure cyber environment. NATO has taken the task of creating cyber security institutions in member countries. India must give concentration to some critical points for cyber security:

- India must raise a Cyber Command. This will comprise not only the three services but personnel from the DRDO and scientific and technological community.
- Government should promote R&D in private industry through active government support for industry-led research projects in the areas of security.
- Strengthening telecom security – one of the key pillars of cyber security.

Make it a mandatory requirement for all government organisations and private enterprises to have a designated Chief Information Security Officer (CISO) who would be responsible for cyber security.