International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

# A survey of Indian Cyber crime and law and its prevention approach

*First A.Angshuman Jana, NIT, Durgapur 1 ; Second B.Kunal Kumar Mondal, NIT,Durgapur 2;*

## Abstract

'Adversary' is a well known term in the cyber security context. The term 'adversary' is used to describe any individual performing or attempting to perform a malicious act. An adversary may be an **insider** or an **outsider**. The term 'insider' is used to describe an adversary with authorized access to a nuclear facility, a transport operation or sensitive information. The term 'outsider' is used to describe an adversary other than an insider. Insider crime presents a unique problem. Insiders could take advantage of their access (i.e. right or opportunity to gain admittance), complemented by their authority (i.e. power or right to enforce obedience) and knowledge of the facility (i.e. awareness or familiarity gained by training or experience), to bypass dedicated physical protection elements or other provisions such as safety. Indian cyber law's are used to protected several illegal activities in cyber place. In spite of that, now it is a crucial challenge to us because day by day crime is gradually increases. This paper introduces some approach to prevent the various cyber crimes.

## Introduction

Computers and their use is a day to day activity of all the students, professionals, teachers, universities, and banks, supermarkets, in the entertainment field, in medical profession and also in higher education [1]. The use of this weapon is spreading vary widely in all parts of our society. As every weapon has two ways of operation. One is good and essential and the other is bad and not essential. Many times, whenever a new weapon is invented, many people use it unknowingly for the wrong purpose. So to aware them and to make the proper use of the power of the newly invented weapon, laws are to be formulated and should be implemented. This chapter introduces the cyber law and many terms involved in it.

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. There isn't really a fixed definition for cyber crime. 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" means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

The word "cyber law" encompasses all the cases, statutes and constitutional provisions that affect persons and institutions who control the entry to cyber space provide access to cyberspace, create the hardware and software which enable people to access cyberspace or use their own devices to go "online" and enter cyberspace [2]. In simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

## What is the Importance of Cyber Laws?

Now a day's do work faster use internet technology, the World Wide Web.Establishing internet individual is difficult for each person in India. So that for people use cyberspace provided this facility. Properly paddle the system need some rule in tram of law. And that law is called cyber law .Cyber Law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace and it help us to protect or safe the system from any unauthorized access, manipulation and catastrophe . Initially it may seem that Cyber Law is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

ISSN:2319-7900

# Various Cyber Crime

Computer crime, cyber crime [4], e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more category. Additionally, although the terms computer crime or cyber crime are more properly restricted to describing criminal activity in which the computer or network is a necessary part

of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used to facilitate the illicit activity. Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with them functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud. Basically above various crimes can happened two ways, outside of cyberspace or inside of cyberspace.

## Technical Aspects

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies from inside (direct attack during system access) or outside (indirect attack via internet) of the cyberspace such as

## Unauthorized access & Hacking

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network [5]. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. By hacking web server taking control on another person's web-site called as web hijacking [6].

## Trojan Attack

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name Trojan horse is popular. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

## Virus and Worm attack

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms.

## E-mail & IRC related crimes

## Email spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

## Email Spamming

Email "spamming" [7] refers to sending email to thousands and thousands of users - similar to a chain letter.

## Sending malicious codes through email

E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

## Email bombing

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

## IRC related

Three main ways to attack IRC are: "verbal attacks, clone attacks, and flood attacks.

## Denial of Service attacks

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

### Examples include

Attempts to "flood" a network, thereby preventing legitimate network traffic attempts to disrupt connections between two machines, thereby preventing access to a service attempts to prevent a particular individual from accessing a service attempts to disrupt service to a specific system or person.

## About insider crime

We generally focus on insider cyber crime. Insider cyber attacks are most dangerous then other attacks because it can happen any legal access of system**.** Further, as individuals having authorized access and with positions of trust, insiders could be capable of defeating methods not available to outsiders. Insiders have more opportunity (i.e. more favorable (conditions) to select the most vulnerable target and the best time to perform or attempt to perform the malicious act. They can extend the malicious act over a long period of time to maximize the likelihood of success. This could include, for example, tampering with safety equipment to prepare for an attempt or act of sabotage or falsifying accounting records to repeatedly steal small amounts of nuclear material. In the discussion of computer security there should be always an assumption that we cannot apply those so called methods or constraints for the employees within. Therefore the insider attacks seem to us like unstoppable. But it is not true always. Insiders can be stopped, but stopping them is a complex problem. Insider attacks can only be prevented through a layered defense strategy consisting of policies, procedures, and technical controls. Therefore, management must pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment. It must look beyond information technology to the organization's overall business processes and the interplay between those processes and the technologies used.

## Types of insider cyber crime

Insiders may have different motivations and may be passive or active, non-violent or violent (Fig. 1). The term 'motivation' is used to describe the motive forces that compel an adversary to perform or attempt to perform a malicious act. Motivation may include ideological, personal, financial and psychological factors and other forces such as coercion. Insiders could act independently or in collusion with others. They could become malicious on a single impulse, or act in a premeditated and well prepared manner, depending upon their motivation .An individual could be forced to become an insider by coercion or by coercing his family members. Passive insiders are non-violent and limit their participation to providing information that could help adversaries to perform or attempt to perform a malicious act. Active insiders are willing to provide information, perform actions and may be violent or non-violent. Active insiders are willing to open doors or locks, provide hands-on help and aid in neutralizing response force personnel. Non-violent active insiders are not willing to be identified or risk the chance of engaging response forces and may limit their activities to tampering with accounting and control, and safety and security systems. Violent active insiders may use force regardless of whether it enhances their chances of success; they may act rationally or irrationally.

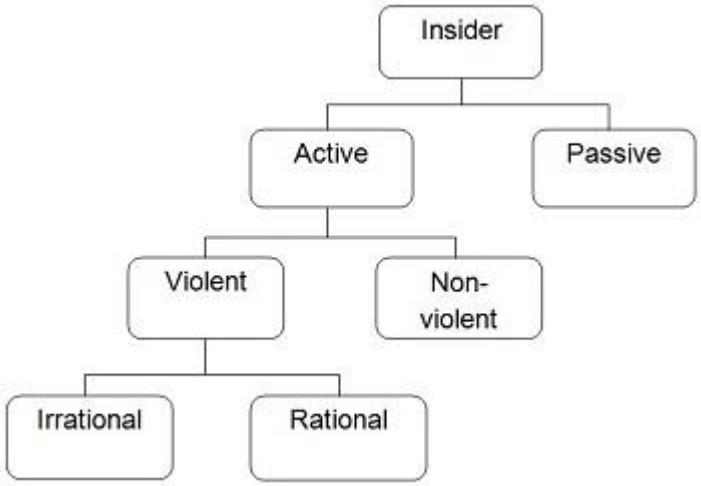


*FIG -1. Categories of insiders.*

## Types of Attacks from Insider

There are many types of attacks can be occur but most importance's are as following:

### Fraud

cases in which current or former customer or contractors intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of

ISSN:2319-7900

obtaining property or services from any cyberspace unjustly through deception or trickery.

## Theft of confidential or proprietary data

Cases involving theft of confidential or proprietary information, in which current or former customer or contractors intentionally exceeded or misused an authorized level of access to confidential or proprietary information from the any cyberspace [11].

## Theft/modification of information for financial gain

## Theft of information for business advantage

Besides these attacks there may be some other thwarts possible that are not convenient to the above scenarios. Some predictions can be made for those:

- Reading executive emails for entertainment.
- Providing organizational (cyberspace) information to lawyers in lawsuit against organization (ideological).
- Transmitting organization's IP to hacker groups.
- Unauthorized access to information to locate a person as accessory to murder. Though there may be more different issues but these are found in the case studies by CERT Program-software engineering team of Carnegie Mellon University. The previous two types of thwart may not be mutually exclusive for a certain case.

# Prevention of Cyber Crime

Prevention [8] is always better than cure. It is always better to take certain precaution while operating the net. The 5P mantra for online security*: Precaution, Prevention, Protection, Preservation and Perseverance.* One should keep in mind the following things-

1. To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.

2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

3. Always use latest and update antivirus software to guard against virus attacks.

4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination

5. Never send your credit card number to any site that is not secured, to guard against frauds.

6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

7. it is better to use a security programmed that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

9. Use of firewalls may be beneficial.

10. Web servers running public sites must be physically separate protected from internal corporate network. Adjudication of a Cyber Crime - On the directions of the Bombay High Court the Central Government has by a notification dated 25.03.03 has decided that the Secretary to the Information Technology Department in each state by designation would be appointed as the AO for each state.

## Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes:

1. Prevention,
2. Detection, and
3. Response.

* User account access controls and cryptography can protect systems files and data, respectively.

ISSN:2319-7900

* Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.

* Intrusion Detection Systems (IDS's) [9] are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

* "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored.

Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. A firewall [10] can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and is normally implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real-time filtering and blocking. Another implementation is a so called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet (though not universal, as demonstrated by the large numbers of machines "cracked" by worms like the Code Red worm which would have been protected by a properly configured firewall). However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place.

# Proposed Practice

A good practice is always '*find the reasons behind the diseases*' i.e. there are reasons behind theft that some customer or other are dissatisfied with something related with organization's(cyberspace) behavior and that drives him to do some anomalous behavior against the particular cyberspace. Some ideas and technologies are proposed below that may be used to prevent insider threats.

## Social Engineering

Actually it is being now days applied in many industries for security. Social engineering is the act of manipulating a person to take an action that *may* or *may not* be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action. It is a huge application of Psychology, behavioral study, cognitive analysis of human behavior. Based on the study, a group of people always be active to motivate the employed guys to do what they should do. They investigate the corner of the user's mind to find suspicious something.

## Secret Team

A secret team is the team who act as customer or other outside user within organizations (cyberspace) but they have another purpose that investigate, monitor or audit the activity of the users. It is like a team of private investigators in disguise.

## Implementing software

Such software should install in each system for every cyberspace that maintain a database of each user or customer. Mainly user or customer details and one unique identification proof issue by government .This software will be maintain by system administer and also invisible with respect to any user or customer. For this approach need extra storages devices. And as per the condition administer will decided how many day's keep information.

## Monitoring the users

Though somebody is newer or recent user, the monitoring is must be needed. It may be by some software (used by system administrator or network administrator) and/or by the security cameras. That means if someone has to steal, then he must overcome a lot of risks i.e. he has to throw dust in the eye of many expertise before flies away.

# Important contents of IT act of India or Information Technology Act 2000

## Preliminary

With the rapid pace, internet usage in India is increasing. So the rule of government is to provide a legal framework for internet and e-commerce.

## Electronic Governance

The filling up of a form, issue of a license or payment of fee may be in an electronic form. Secured digital signatures enable the growth of e-commerce.

ISSN:2319-7900

## Attribution, Acknowledgement and Dispatch of Electronic Records

This chapter of the Act specifies the time of dispatch and receipt to electronic record. An electronic record with a secure digital signature will automatically be considered as a secure electronic record. It will also be considered as a secure if security procedures have been applied to it. Such security may be in the form of encryption.

## Regulation of certifying Authorities

"Certifying Authority" means a person who has been granted a license to issue a Digital Signature Certificate under section24.

## Digital Signature Certificate

It means a certificate issued under sub-section (4) of section 35

## Duties of Subscribers

Subscriber checks any electronic record by means of an electronic method or procedure.

## Penalties and Adjudication

The penalty for tampering source code is imprisonment for a term not exceeding 3 years and/or a fine not exceeding Rs. 200000. In order to enforce the punishments, central government will appoint an Adjusting Officer who will have powers of civil court.

## The Cyber Regulations Appellate Tribunal

The Act contemplates the constitution of the Cyber regulation Appellate Tribunal, having a Presiding Officer. Tribunal will hear appeals from orders passed by adjusting Officer. The party may appeal to High Court of any state within 60 days, if unsatisfied with the order of Tribunal.

## Prevention of Computer Misuse

- Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.
- Each organization shall provide adequate information to all persons, including management, systems developers and programmers, end users, and third party users warning them against misuse of computers.
- Effective measures to deal expeditiously with breaches of security shall be established within each organization. Such measures shall include:

  (i) Prompt reporting of suspected breach;
  (ii) Proper investigation and assessment of the nature of suspected breach;
  (iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach;
  (iv) Remedial measures.

- All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.
- Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:

  (i) The role of the System Administrator, System Security Administrator and management;
  (ii) Procedure for investigation;
  (iii) Areas for security review; and
  (iv) Subsequent follow-up action.

## Use of Security Systems or Facilities

- Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorized users from gaining entry to the information system and to prevent unauthorized access to data.
- Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

## System Access Control

- Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorize issuance of user identification (ID) and resource privileges.

- Access to information system resources like memory, storage devices etc. Sensitive utilities and data resources and program files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.

- The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as “administrator” or “president” or “game” etc. to protect access to the system and data resources represents a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.

## Password Management

- Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:
  (i) Minimum of eight characters without leading or trailing blanks;
  (ii) Shall be different from the existing password and the two previous ones;
  (iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and
  (iv) Shall not be shared, displayed or printed.

- Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

- Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.

# Conclusion

Computer crime is a multi-billion dollar problem. Law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. But still on day’s cyber crime is happening in India. Due to advance meant of technology people apply their multiple or multi-label talent to misuse of technology and also make it harmful to other point of view. So this kind of crime not solved fully by establishing different law, also need to develop human morality, value and ethics proper manner.

# Reference

[1] Cyber Law, Morals & Ethics.
[2] Role of Cyber Law and its Usefulness in Indian IT Industry, Apurba Kumar Roy
[3] New Amendments to IT Act 2000
[4] S. Hinde, “The law, cybercrime, risk assessment and cyber protection”, Computers & Security, vol. 22, issue 2, pp. 90-95, February 2003.
[5] C. Scheideler, “Theory of network communication”, Johns Hopkins University, September 2002.
[6] Adv. Prashant Mali, “Types of cyber crimes & cyber law in India”, CSI Communication, Vol. 35, issue 8, pp. 33-34, November 2011.
[7] Q. Yeh and A. Chang, “Threats and countermeasures for information system security: A cross-industry study”, Information & Management, vol. 44, pp. 480-491, 2007.
[8] A. Bequai, “A guide to cyber-crime investigations”, Computers & Security, vol. 17, issue 7, pp.579-582, 1998.
[9] D. Denning, “An intrusion detection model”, IEEE Trans Softw Eng, Vol.13, issue 2, pp.222-232, 1987.
[10] www.cyberlawportal.com
[11] www.cert.org/archive/pdf/defcappellimoore0804.pdf
[12] http://www.cylab.cmu.edu/

# Biographies

**FIRST A. ANGSHUMAN JANA** received the B.tech degree in Computer Science and engineering from the West Bengal University of Technology, Kolkata, West Bengal,2011. Pursuing M.Tech degree in software Engineering

ISSN:2319-7900

from National Institute of Technology, Durgapur. mail _id - janaangshuman@gmail.com. 9735680336.

**SECOND B. KUNAL KUMAR MANDAL** received the B.Tech degree in Computer Science and Engineering from the West Bengal University of Technology, Kolkata, West Bengal,2011. Pursuing M.Tech degree in Software Engineering from National Institute of Technology, Durgapur. mail_id – kunal.mtech.nitdgp@gmail.com. 9475929208