RAKSHAK FOUNDATION

Prevention of Cybercrime: Issues and Challenges

JULY 2013

Submitted by:

Inderveer Singh

IIT Kanpur

Mentored by:

Shri P V Rama Sastry, IPS

IG, National Investigation Agency

Preface

I am Inderveer Singh, pursuing my B. Tech. in Mechanical Engineering from Indian Institute of Technology, Kanpur. I always have a tendency to seek for better and innovative ways of working and therefore I am quiet interested in developing newer ideas / technologies to solve various day to day problems. Moreover I am also interested in volunteering towards activities for betterment of society and environment in general. My interest has brought me to Rakshak Foundation where I can blend my two interests. Rakshak Foundation engages itself into public policy research matters, moreover it gives college students a chance to do research work on some policy issues and suggest better ideas / solutions / technologies that will directly or indirectly affect society.

Rakshak Foundation, a non-profit organization that is led by a team of highly enthusiastic persons, a majority of them from IIT's all having an urge towards more citizen participation in Public Policy Issues. Since its existence, Rakshak Foundation has worked on many social issues, conducted panel discussions and debates on some of the key issues of our country. Moreover, they have suggested improvements on some of the policies in front of standing committee of parliament also.

In order to bring the youth of country who is interested to work on such issues they conducts summer internship program wherein students from IIT's, IIM's, NLU's and many other prestigious institutions are brought under one roof to work on policy making projects. All the students are assigned mentors who are top-level bureaucrats or professors from academic institutions. Interns have interactive sessions with some of the leaders of society who have contributed immensely towards some social cause. Moreover, interns also have discussions on some of burning issues prevailing in society from technical, legal and social viewpoint.

Acknowledgements

This research work would not have been possible without the support and guidance of many people. Firstly, I would like to thank Rakshak Foundation for providing me this excellent platform to pursue my research on Public Policy Making issues. I would like to thank Shri P V Rama Sastry sir, IPS, IG, National Investigation Agency for taking out his precious time and mentoring me on this project. I would like to thank him for his enriching discussion on some of the important issues and guiding me to experts in this field.

I would like to thank Mr Sanjay Gautam, Inspector, CBI Academy, Ghaziabad, Mr. Omveer Singh, Scientist, CERT-In and Mr S Babu, Scientist, CERT-In for their expert opinion on issues and challenges in the field of Cybercrime. I would also like to thank our coordinators, Ms Nikita Anand, Mr Pritesh Mittal and Mr Siddharth Das for their continuous support and guidance to complete my project work and to organise discussions on some of the current topics of interest of our country.

I would also like to thank all my fellow interns for their continuous support and suggestions to carry research work during the project. I would also like to thank Rakshak Foundation for conducting motivational lectures and sessions by some of the esteemed personalities during the internship period. I would especially like to thank my parents for their continuous support to successfully do the internship.

Contents

List of Tables and Figures

Executive Summary

With the growth of Indian Economy, Information Technology has emerged as one of key sectors contributing to that, nowadays most of the services are available online and computers are becoming a common thing of sight at most of the places. As every coin has two faces, in this context the other face is Rise of cybercrimes. In 2013 it is estimated that the cybercrime business is worth US$100 Billion.

As cybercrime can be done even by sitting in a room and its anonymous nature has resulted in attracting criminals not only for monetary benefits but also to defame someone, threaten someone, to spread their beliefs or even some computer enthusiasts to satisfy themselves by hacking websites.

This report on "Prevention of Cybercrime: Issues and Challenges" gives the overview of the current scenario of cybercrimes in India and ways to make the system more efficient in curbing this menace. Taking into account the

- Types of cybercrimes,
- Vulnerable areas of attacks,
- Awareness among public,
- Specialised Teams for cyber security,
- Legal provisions,
- Jurisdictional issues and
- Good practices guidelines.

This report has been divided into several chapters containing sections and subsections for reader's perusal. First chapter gives an insight into the current scenario of cybercrimes in India, main problems faced by public and investigators, thus defining the goals and objectives of this report. Second chapter deals with the methodology used to conduct research. It comprises of discussions on the basis of the information gathered from all the field visits, literature surveys and meeting minutes with mentor and results drawn out from them. Third chapter gives an

insight into the current government and NGO efforts in this field. Fourth chapter discusses the key findings with gap analysis in the system. Fifth chapter gives the recommendations with their scope and strategy to implement for possible improvement in the efforts to tackle cybercrime. Followed by this are references and appendix having data related to surveys conducted, interviews, field visits and mentor meetings.

The major issue faced by our country is the lack of awareness and there is heavy scope to spread awareness among public. Nowadays children get associated with internet at very early age, so it is very important to have cyber education for children in school curriculum. It is also necessary to spread good practices guidelines among internet users.

Some of the key findings during the research were,

- Lack of awareness about cyber security among majority of internet users,
- Lack of certification mechanism for E-Commerce websites,
- Irresponsible functioning of ISP's,
- Lack of coordination between investigating agencies,
- Lack of trained professionals in cyber security and forensics.

By connecting these dots, some of the key recommendations are

- Awareness Generation Model, this includes strategy to spread good practices guidelines for people in various age groups. Exploiting social media platform for college students, incorporating in school education for children and using print media for elderly persons.
- New specialized teams to tackle cybercrimes and also to conduct awareness generation workshops and seminars. Moreover, these teams will be also responsible for accreditation of websites for security purposes.
- Provision for In-service training of professionals, as the scene of cybercrime is ever evolving. This will also help in fostering the skills of newly recruited professionals.

- Monitoring of ISP's, since these are the entry point of any harmful or unwanted material on internet and they play the key role in tracking cybercriminal. Strict rules to monitor their functioning needs to be brought in place.
- Secured E-Commerce websites, a mandatory certification of these websites needs to be done so as to maintain security of customers using these websites. A rating system based on their security measures can be developed to pressurize them to use better security measures.
- In IT Act, many sections need more precise definitions, as these sections can be misused by criminals or an innocent citizen can be detained.
- Newer Forensic Labs need to be setup since pre-existing ones are already overburdened and due to lack of professionals their efficiency is reduced.
- MoU with higher educational institutions, mutual relationship between government and these institutions will foster development of better software along with creation of newer job opportunities for students in this field.
- Website server hosting in India, special contracts need to be made with companies hosting their websites from other countries to either establish their servers in India or sign a contract to provide relevant information whenever needed by Indian agencies for some investigation purposes.

1. Introduction

1.1 Background Information

Cybercrime, as the name suggests includes all the crimes or offences that include use of computers or associated electronic devices. The late twentieth century, was the time when computers and the internet started gaining power and with the onset of 21st century, computers revolutionized the scene, and now it has become a necessity. Not just mails or Google but from banking to shopping or social networking, with the increased use of computer, it was inevitable for its misuse to also rise rapidly. One form of this is cybercrime, which is so diverse in its nature that anyone can fall prey of it.

Going back one can find that the first case of sabotage was reported as early as 1820. It was not exactly a cybercrime involving computers but a similar one. This is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has also been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access, illegal interception, misuse of devices, forgery and electronic fraud. The World Wide Web or the cyberspace which is spread throughout the world is the place where these

cybercriminals exist; they can attack any person in any corner of the world even without getting traced. Cybercrime has now become an organized activity which is valued up to US$100 billion.

These cybercriminals commit these crimes for either economic or personal motives or to cause reputational damage to somebody. In the present scenario, every person using internet is at the risk of getting affected by some sought of cybercrime. Need of the hour is to have cyber users aware of various threats and how to tackle them.

1.2 Main Problems, their scope and impact on the society

In a single word, the biggest problem with cybercrime is '**Anonymity of Criminal**'. A person sitting in any part of world having access to internet can conduct a cybercrime, even with most basic of skills needed. It becomes very difficult to track that criminal, as a result of this many cybercrime cases remains unsolved. Another reason is that there is no unified policy on cybercrime governing all countries.

In India, in the present scenario the second biggest problem is '**Lack of Awareness'.** India is in a transition phase moving from traditional working models to modern techniques. With the advent of Computers, it is observed that majority of our population is not compatible with this change. As a result of this majority of computer users have vulnerable systems which can be easily targeted and they fall prey of expert cybercriminals.

On cyberspace, the scope of cybercrime is vast with **wide ranging objectives**, like

- Economic
- Defamation
- Personal
- Ideological

Nowadays, there is a huge E-Commerce market being set up on the internet where one can shop, book ticket, avail online banking facilities, play games and many

more. So in this process, one needs to provide confidential information and if the system or that portal is not secure enough then those details can be easily stolen and misused. At times there are cases when people receives phishing mails asking for their banking credentials accompanied with offers of windfall gains and lotteries to lure them. Once such information is provided, there are very high chances of falling prey to economic cybercrimes.

Many a times, due to some personal issues, people also use the internet to defame somebody. Nowadays, there are frequent cases wherein obscene videos are posted on websites which then become viral or false / defamatory information about somebody is presented on social networking websites. Cyber stalking is also becoming a major threat nowadays. Often political / religious / terrorist groups use these tactics to spread their ideology or create panic among general public.

Impact on society is wide ranging, having many dimensions

- Propagation of bad internet practices among youngsters
- Huge monetary losses to person / groups
- Loss to reputation of some person / organization
- Fear of using internet and computers.

1.3 Goals and Objectives

The goal of this project on "Prevention of Cybercrime: Issues and Challenges" is to understand the present scenario of cybercrime in India which includes study of

- Types of Cybercrimes
- Existing laws and legislations
- Awareness among public and precautions taken by them

On a large scale, objective of the project can be distributed into following tasks:

- Concept of Cybercrime, Types of Cybercrimes, Motivations of Cybercriminals and Areas of attack
- Case reports of previous attacks and Consequences of attacks

- Legislations and Legal Provisions for Cybercrimes
- Government policies that are implemented to prevent Cybercrimes, CERT-In (Indian Cyber Emergency Response Team) and its functioning.
- Jurisdictional issues
- Comparison of Indian Laws with International Laws
- List of Recommendations to Government, Amendments in existing legislations and Good Practices Guidelines to internet users and better ways to generate awareness

The recommendations of this report focus on three major areas,

- Prevention of Cybercrimes
- Improvement in Indian Laws (Information Technology Act)
- Better Investigation Techniques

2. Methodology

2.1 Literature Survey

2.1.1 Cybercrimes Study

- Focus is mainly on cybercrimes, their types, their complexity, their areas of attack and the motivation for cybercriminals.[9]
- Doing case study of will give an insight into the modes which can be opted by cybercriminals to breach security, moreover a detailed study of various cybercrimes can be done using available case studies. [22][23]
- Newspaper reports from many national newspapers related to cybercrimes.
- Books on cybercrime / internet can serve the purpose. Using internet to look for definitions will give a broad perspective for any typical cybercrime, while a book may give a single perspective. Lots of blogs by experts on cybercrime are available on internet for detailed study.
- Not all hackers are criminals, so going through various types of hacking that will give an insight into various categories of hackers and their motives.

Literature survey revealed the details of cybercrimes that takes place and case studies gave insight into the consequences of these attacks (Refer section 4.1 of chapter 4 for key Findings from literature survey)

2.1.2 Laws and Legislations Study

In this module we need to look at foreign domestic laws and international laws. A comparison between Indian and International laws can be used to study inefficiencies in Indian Laws. Study of cybercrime statistics gives an insight into the most vulnerable age group, areas of attack and most persistent cybercrimes.

With respect to India, we have

- Information Technology Act, 2000 and its subsequent amendments till Information Technology (Amendment) Act, 2008.
- National Cyber Security Policy, July 2013
- Crime in India, National Crime Records Bureau, Statistics for year 2012

- Data Security Council of India (DSCI) (http://www.dsci.in/)
- Indian penal Code (IPC) for basic crimes that also fall in domain of IT Act

For international laws, we have

- Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL)
- European Convention on Cybercrime
- United Nations Office on Drugs and Crime (UNODC) Comprehensive Study on Cybercrime, Draft, February, 2013

Moreover many reports on cybercrime trends in present scenario can be very useful, like

- Sophos Security threat Report 2013
- Fortinet 2013 Cybercrime Report
- 2012 Cost of Cybercrime Study: United States, by Ponemon Institute
- RSA 2012 Cybercrime Trends Report

2.1.3 Preventive Measures and Awareness Generation

Major reason behind increase in cybercrime is the lack of awareness among the general public. A lot of institutions publish Good Practice Guidelines for specific age group / for specific cybercrime.

- India also has CERT-In (Indian Cyber Emergency Response Team) and CDAC (http://infosecawareness.in/) to look into awareness generation and preventive measures. A study comparing Indian CERT and other organisations with other countries CERT's can be done to formulate better ways to increase awareness among general public.
- FIRST Best Practice Guide Library

2.2 Field Visits and Interviews

Field visits and interviews give an insight into

- The practical scenario of cybercrimes,
- Problems faced by agencies handling cyber security issues in India,
- Loopholes in Laws and their misuse,

- Awareness among general public.

Conducting field visits and interviews at following institutions gives the practical feasibility of ideas proposed

- Central Bureau of Investigation,
- Intelligence Bureau,
- National Investigation Agency,
- Indian Cyber Emergency Response Team (CERT-In)
- Cybercrime Branches of Police
- Cyber Forensics Faculty from several Training Academies

(Refer section 4.2 of chapter 4 for key Findings from field visits)

Survey regarding basic cyber security awareness was conducted among students from colleges (got 200 responses), (Refer section 7.3 of chapter 7 for results of the survey). Moreover a more diverse survey can be conducted taking into account different age groups and awareness level among them.

2.3 Mentor Meetings

Mentor meetings played elemental role in setting the direction for research and getting contacts of experts working in this field. Expert opinion is a must while working on issues which were revealed from field visits and needed attention and analysis. Some of the major benefits of mentor meetings are:

- Setting up agenda for the project and key areas to be focussed,
- Strategy for effective implementation of recommendations proposed,
- Guidance while comparing Indian Laws with International Laws,
- Mechanism for Awareness Generation Model.

3. Government and Current NGO Efforts

3.1 Government Efforts

- **Cyber Crime Cells / Branches:** At present police has established a number of cybercrime cells, their responsibility is to disseminate warnings/ alerts about threats prevailing on internet, have a portal for online complaint registration, they have their helpline numbers and issue good practices guidelines. These cells have experts on cyber forensics and they look into specific issues related to cybercrime. It is mandatory for each district's police department to have one cybercrime cell.
- **CERT-In (Indian Cyber Emergency Response Team)**: CERT-In is the national nodal agency to look into issues related to cyber security. CERT-In shall be performing the following functions in the area of cyber security:
    - Collection, analysis and dissemination of information on cyber incidents;
    - Forecast and alerts of cyber security incidents;
    - Emergency measures for handling cyber security incidents;
    - Coordination of cyber incidents response activities;
    - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
    - Such other functions relating to cyber security as may be prescribed.

  Moreover CERT-In also conducts workshops and trainings at various levels to train professionals working on cyber security issues. It also looks into investigation and cyber forensics. It collaborates with various other investigation agencies in our country to look into issues related to cyber security. It also publishes good practices guidelines related to internet usage.
- **Information Technology (IT) Act, 2000:** This act was passed to provide legislation in the field of Information Technology and combat with the increasing issues related to cyber financial frauds / theft and to handle issues of defamation using electronic medium. This Law didn't had proper

definitions for lot of newly emerging cybercrimes, so in order to tackle that many amendments were made in the law and an amendment act was passed in 2008.

- **National Cyber Security Policy(July 2013):** Recently this policy has been launched to tackle increase in cybercrimes in our country and to strengthen the implementation of Laws related to Information Technology. Some of its salient features are:
    - National Cyber Alert System,
    - Sectoral CERTs and Local Incident Response Teams,
    - Implementation of security best practices in government sectors,
    - Security crisis management for countering cyber-attacks,
    - Developing Better Technology,
    - Awareness Generation and Enabling Citizens.
- **Awareness Generation:** Government has also taken some initiatives to generate awareness among the internet users, in collaboration with **Centre for Development of Advanced Computing (CDAC)** they have made portals that issues good practices guidelines, this is done with the help of posters, cartoons, comic strips, etc.

3.2 NGO's working in the Field of Cybercrime

At present, in India there is less public participation on cyber issues. Some of the NGO's working in this field are:

- **The Centre for Internet and Society:** The Centre for Internet and Society is a non-profit research organization that works on policy issues relating to freedom of expression, privacy, accessibility for persons with disabilities, access to knowledge and IPR reform, and openness (including open government data, free/open source software, open standards, open access to scholarly literature, open educational resources, and open video). It also engages in academic research on digital natives and digital humanities. They mainly focus on accountability for content on internet and how internet can contribute towards strengthening the bond between various sections of

society. Through multidisciplinary research, intervention, and collaboration, they seek to explore, understand, and affect internet, and its relationship with the political, cultural, and social milieu of our times. They also have forum for debates on such issues and also publishes articles on such issues.

- **Cyber Crime Complaints (CCC):** CCC is a website where we can write any of our complaints about cybercrime; it also issues information to present threats and issues guidelines.
- **Techgoss.com:** It is also one of the sites that gives information on the present vulnerabilities present in cyberspace and also issues warnings, moreover they also have debates and articles on policy matters related to cyber security.

4. Results and Discussions

4.1 Findings from the literature

From literature survey and theoretical reading on cybercrime, the main findings were:

4.1.1 Motivation for Cybercriminals

1. **Economic:** This includes the cybercrimes that are committed to get economic benefits. They try to get confidential financial information, directly ask the victim to send some money or they may get access to victim's computer system and extract confidential financial credentials. These includes: Phishing mails, Credit card frauds, network scanning / probing, false digital signatures, email bombings on security systems of banks, online gambling, pornography and sale of illegal articles.
2. **Personal:** Some cybercrimes are committed to satisfy oneself for some personal reasons. These may be crimes committed due to Personal Vendetta; Blackmailing; Ego, Mental Aberrations; Mischief; Sexual Gratification; Stealing vital secret information; Destroy, Damage or change vital computerized control systems at various installations. These may include cyber stalking, spamming, denial of service attacks, hacking or sending virus / malicious software.
3. **Reputational Damage:** In these cybercrimes main motive is to defame somebody's image. This can have adverse effects on victim leading to mental or physical damage. These include sending obscene material via mails, MMS or uploading them on websites, email / social networking profile hacking and defacing of websites.
4. **Ideological:** The cybercrimes having ideological motives behind them to threaten public or create panic among them comes under this domain. This includes Hactivism and sending threatening mails (cyber terrorism)

4.1.2 Type of Hackers / Crackers

1. **White Hat (ethical hackers):** A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while

working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council, also known as the International Council of Electronic Commerce Consultants, is one of those organisations that have developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.

2. **Black Hat (cybercriminals):** A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. They choose their targets using a two-pronged process known as the "pre-hacking stage".
3. **Grey Hat:** A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.
4. **Blue Hat:** A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue Hat to represent a series of security briefing events.

4.1.3 Cybercriminals

1. **Professional Hackers and Crackers:** Hacking in simple terms means illegal intrusions into computer system or network of other persons or organizations. Hackers write or use ready computer programs to attack the target computer. Hackers are proficient with computers and programming to elite level where they know all of the ins and outs of a system.
2. **Children and Adolescents:** The children resort to this type of delinquent behaviour pattern mostly due to the curiosity to know and explore the

things. Other equivalent reason may be to prove themselves to be outstanding amongst other children in their group. Further, even the psychological reasons may be there.

3. **Professional Hacktivists:** These kinds of hackers are mostly organized together to fulfil certain objective. The reason may be to fulfill their political bias fundamentalism, etc. Also, these may be well funded too. They usually indulge in the defacement of websites or the hijacking of websites by redirecting traffic to a spoof website. The hacktivist groups usually target government websites, international or multinational organisations and financial institutions.
4. **Greedy / Disgruntled Employees** This group includes those people who have either been sacked by their employer or are dissatisfied with their employer. Such employees prefer to adopt illegal means to increment their salary with large sum of money or for the sake of avenging. Especially the temporary employees often succumb to the goddess of the quick buck. They normally hack the system of their employee or post defamatory material about him / her on the web. Till now they had the option of going on strike against their bosses. Now, with the increase independence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes.
5. **Dejected Lovers:** Another set of cyber criminals include dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their desires. Often they resort to crime of cyber stalking to disturb their beloved. Besides they also try to hack their e-mail ID's to know if the person is going around with someone else. They often hack their profiles on social networking sites to defame them. Usually such criminals are not experts and may get caught easily if reported.
6. **Computer Pirates:** Computer piracy is a distinct kind of cybercrime which is perpetuated by many people online who distribute illegal and unauthorized pirate copies of software. Computer pirates are those cyber criminals who steal valuable property when they copy software, music pictures, movies, books available on the internet. There are many P2P (peer

to peer) file sharing software program in the market with the help of which they can easily copy and exchange software, movies, music downloads, book etc. on the internet. However, most of this material is copyright protected which means that one is restricted from making copies unless he / she has purchased the same stuff. However, this criminal offence occurs every day on computer systems around the world including the internet. This is a very serious problem and is very difficult to circumvent.

7. **Sex Maniacs:** Internet is full of online sex maniacs who perform variety of illegal activities like pornography, child pornography, production, possession, distribution or transmission of sexual material and including minors for sex over internet etc. Although some offenders have adopted illegal activities like pornography as their industrial business, sex maniacs do it primarily to satisfy their lust. In fact these offenders are responsible for corrupting minds of others and further making them sex maniacs too.
8. **Spies:** Cyber espionage has become very common since the industrial revolution. Industrial espionage is on increase because of the expensive reliance on the computer systems and networks to document industrial plans, projects, experiments and research. Such spies are hired by the industries quite often these days. It is motivated by money as it is a well-paid activity and sponsor stands to gain knowledge worth millions of dollars at minimal expense and minimal risk. Also, the gathering of military and other intelligence is done by governments, organized criminals guerrillas and terrorists.

4.1.4 Variety of Cybercrimes

1. **Phishing:** Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often

directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

2. **Spamming:** Spamming is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, social networking spam, social spam, television advertising and file sharing spam.
3. **Denial of Service (DoS):** Attempt to overwhelm or overload the organizations website, network by which it becomes unavailable to the outside world. This is generally done by increasing the unwanted traffic on that website making it unavailable for the intended users, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers.
4. **Website Defacement:** Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. Defacement is generally meant as a kind of electronic graffiti, although recently it has become a means to spread messages by politically motivated "cyber protesters" or hacktivists. It is generally done by means of SQL injections which allow gaining administrative access.
5. **Internet financial fraud (Digital Forgery):** This cybercrime has many forms and very diverse in nature viz., **credit card frauds, financial credential theft, false digital signatures, internet auction fraud and fraudulent transactions**. These are the ones that generally gain a lot of attraction since initially cybercriminal lures the customers for heavy benefits then cheat them, this may be done by asking users to send financial

credentials online or by filling details on fake transaction portals, creating false digital signatures for unauthorised access to others accounts. It also includes large transactions in short amount of time done by using malicious codes and unauthorised breaching in the security of bank's websites

6. **Cyber Defamation:** Some persons use various means to defame some person by posting hateful or misleading comments, defaming the concerned person. It may be due to personal grudge against that person.
7. **Identity theft:** Some cybercriminals uses different tactics to get access the other person's account by stealing their account credentials this can be done by predicting their passwords, by exploiting loop holes in the security of their account, by phishing mails or even by phishing pages. Identity theft can be done for various purposes like cyber defamation or to send unauthorised material online. It is generally advised to set strong passwords to avoid identity theft and avoid filling confidential information on unknown pages.
8. **Theft of internet hours:** Theft of internet hours refers to using up or utilizing of somebody else's Internet Services. In many cases, when a person takes up the services of any internet service provider, he utilizes the services in terms of number of hours consumed and makes the payment on a per hour basis, whereas unauthorised use of these services in a crime.
9. **Virus / malware / malicious code:** This is the biggest threat to any person using internet, in this unwanted harmful software contaminate your computer and may lead to severe results. There may be different reasons for such virus / malware and are known by many names, viz. worms, Trojan horses, ransomwares, keyloggers, etc. some of them may just corrupt your files, some may hijack your system and then your system may work according to some other persons instructions **(Bot-net infection)**. Severe outcomes may even lead to disruption of power grid system or working of industrial plant.
10. **Cyber Stalking:** Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements

of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass.

11. **Online gambling / gaming:** Nowadays, it is very common to see games having virtual money to play online, with players from different countries. By any players winning or losing their money gets transferred through the agents across countries illegally. This is a crime as it violates FARA (Foreign Agents Registration Act)
12. **Sale of illegal articles:** Illegal articles like animal fur, weapons, drugs, pornographic data, etc. are not allowed to be sold by any means and doing these transactions also comes under cybercrime.
13. **Cyber pornography:** Showing of obscene or sexually explicit material over internet comes under the domain of cyber pornography. On cyberspace there are lots of sites available where this content can be viewed anonymously. There are many forms of porn available ranging from child pornography to adult pornography.
14. **Spoofing:** In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Some websites, especially pornographic pay sites, allow access to their materials only from certain approved (login) pages. This is enforced by checking the referrer header of the HTTP request. This referrer header however can be changed (known as "referrer spoofing" or "Ref-tar spoofing"), allowing users to gain unauthorized access to the materials.
15. **Network scanning / Hacking:** It is generally used by the cybercriminal to get access to others computer and then scan that system for relevant information. It goes through step of processes, viz.,

- **Vulnerability scanner:** A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version

number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented).

- **Password cracking:** Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.
- **Packet sniffer:** A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.
- **Spoofing attack (Phishing):** A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.
- **Rootkit:** A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

16. **Hacktivism:** In simple words, it means politically motivated technology hack. A group of people targets some website, generally political or government website and starts bombing it with mails, until it goes out of service. Many a times this mail contains messages to convey their ideology against that website owning community's belief.
17. **Cyber terrorism:** It is a controversial term, as it may include all the activities that support some sort of terrorism. Mainly websites hosted by terrorist groups are already banned but any activity that may harm the

sovereignty of any country or is used to threaten or create panic among the citizens may be regarded as cyber terrorism.

18. **Stenography and Cryptography:** With respect to cybercrime, it includes ways by which messages can be encrypted in some other form so that they can't be read by some other person. Sometimes these methods are used to transmit messages that may be used to do some illegal activity. It is very hard to detect such messages.
19. **Unauthorized IP use:** In India it has been seen that many government offices and universities use open proxies and does not have any security measure taken to prevent its unauthorized use. Due to this reason these IP addresses are used by unauthorized people (even by Cybercriminals) for wrong uses. Such open IP's are common sites of attack for cyber criminals. Many a times such IP are used to send unauthorised messages or cybercrimes are committed. It is a crime to maintain poor security measures for any Wi-Fi server created by any person.
20. **Sabotage:** Sabotage is a deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction. In a workplace setting, sabotage is the conscious withdrawal of efficiency generally directed at causing some change in workplace conditions. These type of attacks target a website and by either increasing the unwanted traffic too much or by defacing it, makes that website unable to work properly.

4.1.5 Laws and Legislations: IT Act, 2000 and its amendments till IT (Amendment) Act, 2008 are the only laws governing cybercrime in India. From theoretical analysis and case studies, these were some of the findings:

- **Section 67 B:** Child Pornography is the topic that has not been dealt accurately and various forms of pornography in which adults imitate child or drawings depicting children in pornographic activities have not been defined.
- **Section 66F:** This section deals with cyber-terrorism. The law uses some terms that have no proper definition with respect to the context. Terms like

decency and morality are used which can be easily used for vested interest of some persons.

- **Lack of Definition of Abuse:** In our laws, at many places discussions have been done with respect to offensive / abusive terms used on internet. But still no laws exist to define what is abusive, as it may be abusive to one person but not to other.
- **Jurisdiction Issues:** In IT Act,2000, Sec. 75 does says that all the laws holds even when the criminal is from some other country, but in reality India needs to have a treaty for mutual sharing of information with other country in case of any international cybercrime.

4.1.6 Preventive Actions: In India institutions like CERT-In and CDAC are at present working in the field of issuing warnings / alerts about the threats present in cyber space and also to issuing good practices guidelines for internet users. CERT-In office is situated in New Delhi and as a result of this people from far places are unable to get in direct contact with CERT-In and most of the people on internet are unaware of CERT-In and similar is with CDAC, they issues good practices guidelines in user friendly form specifically for children and adults, but majority of them are unaware of these steps taken by government and fall prey of prevailing cybercrimes.

4.2 Finding from the field Visits and impact on the theoretical focus of the project

Field visits and interviews revealed a lot of things that which were not highlighted by literature analysis. Some of the key findings were:

4.2.1 From Public Point of View

1. **Awareness among public:** Most of the internet users are unknown of basic security measures. People often use pirated software and they are unsecured. It often seen that people have weak passwords, moreover they discloses their passwords. They easily get attracted towards fake mails about lottery's and

auction without even checking the authenticity of concerned person. Very less steps are taken from prevention point of view.

2. **Unauthorised use of IP Addresses:** In India it has been seen that many government offices and universities use open proxies and does not have any security measure taken to prevent its unauthorised use. Due to this reason these IP addresses are used by unauthorised people (even by Cybercriminals) for wrong uses.
3. **Cyber Café Guidelines:** As per IT Act, 2000, any person who provides internet service must follow some guidelines and rules, but a majority of them does not follows, they don't have their own servers so that they can keep track of the websites used by the customers. This may lead to a punishment for 3 years, but no step is taken by government to keep a check on it (they only comes into effect when some incidence takes place).

4.2.2 From Government Point of View

1. **Unavailability of Private IP address; Problem in tracking criminals:** Most of the ISP's does not provide their customers with private IP addresses; in general they have more than 100 persons for each single public IP address. This is because while government make contracts with these companies, there was no such clause in contract. Major disadvantage is that when some person has committed some crime, then while tracking that person, it is very difficult since those 100 persons under single public IP may be distributed throughout the country and that creates a challenge to track actual criminal.
2. **Irregularity in blocking foreign country's harmful websites:** There are many websites which uses open proxies, shows obscene material and can be used to send anonymous mails. It is even harder to get data from these websites hosted in other countries, during investigation of cases. Government should take strict measures to identify and block these websites in our country. Steps must be also taken to prevent all the virtual money transactions going in cyberspace, as it is violation of FARA.
3. **Difficulty in making agreement:** India does not have a mutual agreement related to cybercrime with countries and as a result of this, if we want to get

any data, we are unable to get it since most of these company's servers are in other countries. Countries like USA and China have made effective agreements in terms of cybercrime.

4. **Lack of Company's servers in India:** Many companies do not establish their servers in India, to avoid the increase in investment in our country. As a result of this, if we need any data from these websites, we need to get it from some other country hosting the server. If we don't have any ties with that country, we cannot get access to require data. The main loop hole is the contract that is initially signed with the company**; it does not contain any clause for establishing their server in India**. It must be noted that while making any contract with a company, a clause regarding setting up of server in our country must be present in it.
5. **Provision for CERT-In nodal branches at state level:** Steps must be taken to make CERT-In more active, this can be done by establishing nodal offices of CERT-In at state level, new recruitment for trained professionals must take place and each nodal centre must be responsible for solving regional issues and spread awareness among public, also about the misuse of their network by other people. This must be done by organising seminars and workshops at educational institutes.
6. **Lack of Knowledge at Sub-Inspector level in police:** Sub-Inspector is the first person who responds to the complaints of people. But according to Sec. 80 of IT Act, 2000, Inspector is the lowest level of officer that will deal with issues of cybercrime and majority of inspectors and sub-inspectors don't have adequate knowledge in cybercrime, as a result of this very few cases of cybercrime gets registered. Steps must be taken to train inspectors about cybercrimes and IT Act's provisions. Even after registering cases the defence lawyer has upper stand since police officers lack proper knowledge regarding cybercrime and their legal provisions.
7. **Cyber terrorism: Anybody can be arrested:** Lack of accurate definitions of many terms viz. injury to decency and morality, may lead to life imprisonment, here decency and morality have no accurate definition. In order to stop misuse

of this section 66F of IT Act, 2000, steps must be taken to elaborate upon issues of cyber terrorism.

8. **Lack of definition of abuse:** The need of the hour is to create a database of abusive terminologies after consultation with people of different places and backgrounds. For eg. word 'Chutia' is surname of people in Assam but it also an abusive word in many parts of our country, so a person sitting in US can't decide on whether it is abusive or not. Government should come forward and take actions on making decisions regarding abusive terminologies propagating on internet.
9. **Power to police**: In order to track tentative criminals and prevent subsequent crimes, police must be empowered, for eg. in order to catch criminals involved in sending obscene materials, police must be allowed to make fake social networking profiles and subsequently catching the criminals. Moreover, there must follow-up sessions for such criminals to tell the police station about their whereabouts after completion of sentence, also police can keep an eye on them.
10. **Lack of proper definition of Pornography vs. Child Pornography:** In India, it is an offence to view or transmit child pornography (involving persons below 18 years of age), but in case of adult pornography, it is illegal to transmit it but legal to view it. Government must take adequate steps to block such websites in India, make viewing adult pornography illegal and also take strict actions against people involved in this business
11. **No proper cybercrime related agreement with countries:** India have agreement with very few countries on issues of cybercrime. As in European Union countries, India must also sign treaties with countries to solve issues of international cybercrimes.
12. **Improper security measures to deliver confidential information by government:** There are lot of government websites which have inadequate security measures and confidential information can be leaked out easily. For eg. Income tax E-filing website can be used to get PAN numbers of persons by having minimal information and can be used to make fake PAN.
13. **No software development agencies in India:** In cyber forensics, some software with specific features are required and in the present scenario our

government is buying these software from foreign countries that are made for their specific need, so sometimes it also goes ineffective in investigation of some cases. Government must collaborate with technical institutions in our country to develop software by taking feedback from investigation agencies. This will not only lead to effectiveness in investigation but also in reduction of expenditure.

14. **Lack of Professionals:** The present situation with Indian investigation agencies is that there are few trained professionals to combat cybercrime. Officers at higher posts (decision making positions; even in-charge of cybercrime branches) also lack necessary skills needed to tackle cybercrimes, due to this these branches does not work efficiently. It is needed to bring professional lot of people in investigation teams or there must a training program for even lowest level officer.
15. **Lack of motivation for professionals:** In the present scenario, even trained professionals have no incentives to work in government agencies since there is lot of hierarchy order in offices and in most situations higher post officers are not professional, so the work done by lower officers gets inadequate response, thus leading to demotivation.
16. **Signing Mo U's with IIT's and NIT's:** Government must come forward and sign MoU's with good technical institutes of our country, this may include development of software by their students, discussions on improving cyber security, introduction of courses on cyber security and development of good practice guidelines for general public.

4.2.3 From Cybercriminal Point of View

1. **Use of Multi-Proxy:** Many of the cyber criminals have started using multi proxies these days, by this they gets access to internet from an IP address in one country (say A), then opens browser by another IP address in other country (say B), then uses open proxy of a third country (say C) to send some wrong message. In these cases it is very **difficult for investigators to track location of such criminals** and also the legal ties between these countries are a matter of concern while investigating such cases.

4.3 Gap Analysis

- **Lack of Professionals:** For handling cybercrime issues, persons with expertise in computer science / information technology are required. It was observed that that there is lack of trained professionals in majority of government departments handling cybercrime issues. Due to this reason, majority of cybercrimes remains unattended or unsolved. This is also a reason that very less cybercrimes gets reported (~5%). Due to this a lot of time and efforts gets wasted training these untrained professionals. Even CERT-In is having courses for cyber auditing, people are unaware of that.
- **No Awareness among public:** Even if government is taking appropriate measures to combat cybercrime, majority of cybercrimes takes place due to mistakes committed by public. Almost 95% of financial frauds take place due to confidential data getting leaked through phishing mails. People in different age groups uses internet for different purposes and they don't have knowledge of existing threats on internet. Good practices guidelines are not known to public. Nowadays child uses computers at very early age, and there is no cyber education for them in our education system.
- **No Local Agencies / Teams:** All the major agencies dealing with cybercrime are situated in major cities but there are no agencies to look into cybercrimes at local level. It delays investigation of many cases and increases work load on nodal agencies at national level. Also there are many local issues like cyber café monitoring, monitoring of sale of SIM cards and control over unsecured open proxies cannot be done unless there are local agencies.
- **Irresponsible Functioning of ISP's:** At present ISP's does not take any steps to filter harmful / improper content on internet. Moreover, sale of SIM cards is done in unaccountable manner and due to this in many cybercrime cases fake SIM cards are used. When ISP's are asked to provide logs / data during investigation process, they provide them in unorganized manner without any specific format, which leads to excess wastage of time and efforts in order to sort out these logs.
- **Problems in Coordination between Public and Law Enforcement agencies:** In IT Act, inspector is lowest level officer to register any FIR under IT Act but at

majority of police stations Sub-Inspectors are responsible for registering FIR's. This leads to lack of coordination between victim and police. Moreover, senior officers at these police stations have less knowledge about cybercrimes and IT Act, thus many cases of cybercrime does not gets registered.

- **Excessive Work Pressure on Forensic Labs (FSL's):** At present there are very less forensic labs in our country and during investigation of most of cybercrime cases FSL's needs to do evidence analysis. With increase in number of cybercrimes, it is becoming very difficult for FSL's to handle all the cases effectively and investigate them accurately.
- **Improper Transfer policies for Cybercrime branches:** It is observed that in most of Cybercrime Branches, officers who have either very less or no knowledge of information technology are getting transferred. It takes them additional efforts to get trained in this field. This generally leads to reduction in proper functioning of these branches. Also trained professionals are transferred in normal police stations thus leading to decrease in cyber security workforce. This leads to gradual demotivation of professionals. It is necessary to have specialised policies for cybercrime branches so that professionals goes to correct place.
- **Lack of Courses on Cyber Security in Technical Institutions:** Very few Technical Institutions in India have courses on cyber security or forensics. As a result of this, students are unknown to this aspect of their studies. Due to reduced number of trained professionals in this field, there is a lack of good quality software related to cyber forensics; moreover, most of the software currently in use for this purpose is imported from other countries. They lack efficiency in our country since they are made for that country's specific purpose.
- **Loopholes in IT Act:** In the amendment act, positive steps have been taken by government to make the Law more effective by bringing in idea of electronic signature rather than digital signature. Even after this proactive attempt by government, there are some sectors in Act which needs further analysis, these are:

- **Child Pornography:** Though this section has been drafted with some care but still some intricacies are not well addressed. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the section, it is unclear whether drawings depicting children will also be deemed an offence under the section. Regarding the age of differentiating a child from an adult, it has been mentioned that 18 years is the limiting age but in section 67B age of children is being defined as older than the age of sexual consent. This needs to be reframed.
- **Transmission of obscene material online:** In sec 67, 67A and 67B, the phrase "Causes to be transmitted" is used. It would mean that the producer, the recipient and the the person from whose server the data has been sent will all be charged for it. Steps need to be taken to strengthen it and this can act as a cap on transmission of obscene material online.
- **Offensive Messages (Section 66A):** There needs to be a strict definition for type of offensive material. The fact that some information is "grossly offensive" or it causes "annoyance" or "inconvenience" while being known to be false cannot be applied to everything. But issues related to decency, morality, public order or defamation must be handled carefully under this section.
- **Blocking of Websites:** There is no specific guidelines or process regarding blocking of websites. Any material available on internet that is harmful to public (or person in specific) is liable to be blocked by government. But in order to tackle the issues of internet censorship, there must be some governing board or team that must look into details of blocking websites.
- **No provision for monitoring of E-Commerce Websites:** IT Act does not have any section regarding certification mechanism for websites having monetary transactions online. Moreover there isn't any provision regarding the minimum necessary security measures that needs to be incorporated by these websites.

- **Cyber Terrorism:** Section 66F (1)(B), defining "cyber terrorism" is much too wide, and includes unauthorised access to information on a computer with a belief that that information may be used to cause injury to decency or morality or defamation, even. While there is no one globally accepted definition of cyber terrorism, it is tough to conceive of slander as a terrorist activity.
- **Penalties:** Most of cases having offences carrying penalties above three years imprisonment have been made cognizable, they have also been made bailable and lesser offences have been made compoundable. This is a desirable amendment, especially given the very realistic possibility of incorrect imprisonments (Airtel case, for instance), and frivolous cases that are being registered (Orkut obscenity cases). There must be more analysis on which offences must be made non-bailable and rest bailable.
- **Cheating by personation:** It is not clear whether it refers to cheating as referred to under the Indian Penal Code as conducted by communication devices, or whether it is creating a new category of offence. In the latter case, it is not at all clear whether a restricted meaning will be given to those words by the court such that only cases of phishing are penalised, or whether other forms of anonymous communications or other kinds of disputes in virtual worlds (like Second Life) will be brought under the meaning of "personation" and "cheating".

Some of these issues have been addressed in National Cyber Security Policy, 2013, but main hurdle lies in successful implementation of changes proposed.

5. Recommendations, Scope and Strategy for Implementation

5.1 Awareness Generation Mechanism

Scope: During literature analysis, field visits and surveys conducted, it is observed that there is a need to generate awareness on cyber security issues, since 70% of all cybercrimes take place due to some mistake done by victim. Since majority of victims of cybercrimes are youth between age of 18-30 years, so we need to specifically target population in this age group and the ones entering into it in near future.

Strategy for Implementation: The institutions working in the field of awareness generation like CDAC and CERT-In can consider this mechanism as a pilot project to implement similar models to all India levels:

1. Generate job vacancy for persons qualified in computer science / Information Technology with any of these degrees B.Tech. / M.Tech. / B.Sc. / M.Sc. / BCA / MCA for the position of trained professionals in the field of Trained Certified Cyber Auditors and Cyber Security Training Professionals. Training of these candidates will be done by these mentor institutions. These will be **1st Tier** professionals.
2. Now that we have the trained professionals, we can start with step 1, that is Cyber Security Workshops / seminars in Colleges and Institutions on Hacking / Threat analysis, training of teachers in schools and generation of **2nd Tier** professionals for running private government funded courses in computer training and cyber security (summer courses and workshops).
3. Now that we have 2nd tier of trained professionals, information can be dissipated more effectively to the lower strata of computer users(**3rd tier**); those are school students, old aged people and corporate users. Mock training sessions can be organized for them in order to assess their grasp of course material.
4. Use of Social Media: This step is to be implemented before previous step, now, step1; using facebook and twitter create pages and profile (say, cyber security Team India). Why before step 1, so that we can link our students during

workshops to these pages and profiles. These profiles will have various posts like, Cybercrime case studies, Cyber Security Tips, Good Practices Guidelines, Present Threats and Vulnerabilities on Cyberspace and organize competitions related to these issues. Target is to make this page is to have impact on public, make it more informative for people and keep them interested towards it (as if these are celebrity pages).

5. Use of Print media: This mode is used to reach out to the people who cannot access / are not accessing the above mentioned modes, articles about cybercrime incidents in newspapers can prove to be informative for aged / working people. These articles can be used to spread good practices guidelines in order to avoid such incidents with the reader. For housewives and secondary school children, we can have comic strips and articles in common magazines / comics.
6. Cyber Education as a part of School Curriculum: Nowadays, internet is used by children at very early age. In order to teach them about cyber good practices guidelines, involving cyber education in curriculum can bring about a change in their behaviour. This will create an aware and empowered youth for next generation. Moreover, children using internet will also learn some internet atticates.

Flowchart:

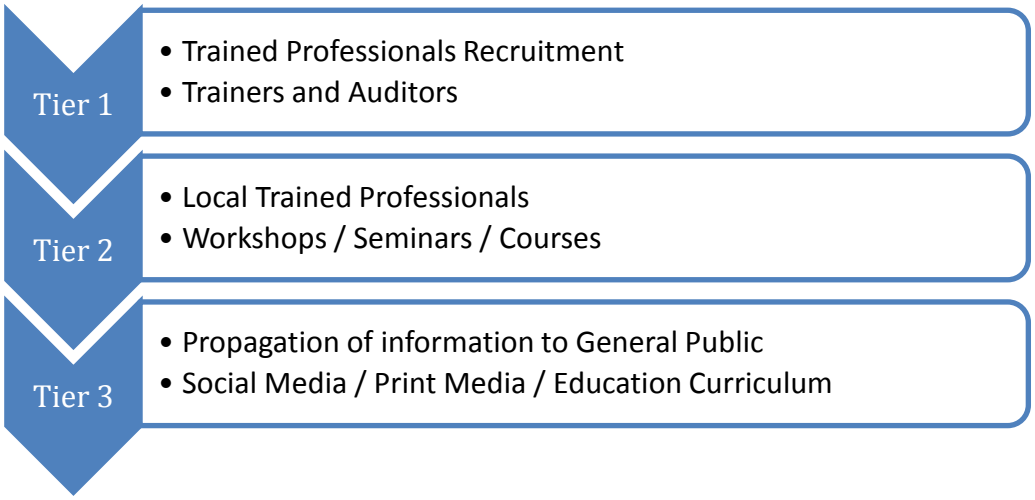


Fig 1: Awareness Generation Model (Tier Structure)

Fig 2: Implementation mechanism for Awareness Generation Model

5.2 Certification of E-Commerce Websites

Scope: In the present scenario, financial transactions over E-Commerce websites are very common. In these transactions, users don't know that the credentials submitted by them are actually secured or not. Many a times they get lured by huge discounts / offers made by these websites. If we have a system of certification of websites based on security measures taken by them and rating them on basis of certain parameters and if such a database is maintained then, it can be of great convenience for customers to use a secured website, thus contributing to reduction in online financial thefts.

Strategy: All the E-Commerce websites must undergo a mandatory certification process to conduct cyber security audit of their website so as to accredit their website. This cyber security audit will give the website owner information about various vulnerabilities on website and will be rated accordingly. So in order to attract crowd on its website, they need to improve their security measures and improve their rating. Thus having improved security measures for these websites.

Flowchart:

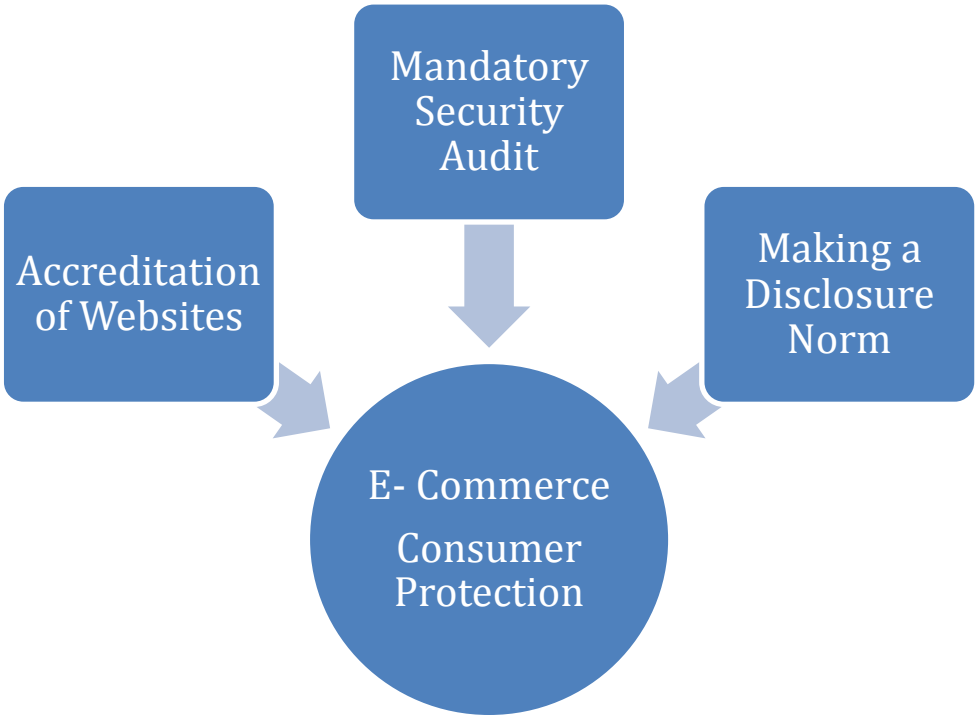


Fig3: Benefits of Certification of E-Commerce Websites

5.3 Monitoring of ISP's

Scope: Internet Service Providers (ISP's) are the end terminal to provide internet to users. This is done by providing an IP Address to the user (through SIM card / Modem / Broadband). Whenever some cybercrime takes place, ISP's are contacted to get the details (Logs) of culprit's and victim's IP address. Three major problems are faced by investigators,

1. No supervision over sale of SIM cards,
2. No standard format for providing logs thus making it hard to retrieve data,
3. No filtering of data (that may be harmful).

As a result of these cases either gets delayed or remains unsolved. ISP's must be monitored more accurately to facilitate investigation and increase their accountability.

Strategy:

1. All the ISP's must have strict provision on sale of SIM cards. In order to avoid misuse of credentials of customers by local vendors, there must be a strong checking mechanism to be implemented by these ISP's. Now, how to force ISP's to implement such policy, in IT Act, a clause must be added in which ISP's must also be made responsible for any crimes committed by their network.
2. ISP's must be instructed to block those websites that are notified by respective authorities to be harmful.

5.4 Specialized Teams for Cybercrime

Scope: At present there is a lack of professionals to deal with issues related to cybercrime and cyber security at local levels. We need have more decentralized teams to look into issues like,

- To conduct mandatory certified audit of websites
- To conduct investigations at local level, as CERT-In and CBI are institutions at national level, they are unable to go for investigation for majority of cases
- To conduct workshops and seminars in educational institutions / schools
- To look into various means to generate awareness in that region
- To register cases regarding cybercrimes (preferably online)

Strategy: Recruitment of IT professionals and training them for cybercrime investigation, prevention mechanisms and for certified cyber security audits. Now, there must be different sections of team that looks into

- Awareness generation,
- Cyber security audits,
- Investigation and cyber forensics,
- Analysis of current trends in cyber threats in cyberspace,
- Monitoring of cyber café and open proxies / unsecured WiFi networks in that region,
- To look into issues that need international jurisdiction.

Outcome: At present central authorities can't look into so many issues throughout the country, but by the presence of such teams, these issues will be more effectively handled at local level. Moreover, central agencies can look on the functioning of such decentralized institutions.

5.5 In service training for professionals and Specific Transfer Policies

Scope: In case of cybercrimes, mode of attack gets modified almost every day; with a new threat getting generated there is a need to develop newer technique to crack it. Now, officers in cybercrime branch who are trained some time back faces problem in tackling such newer threats due to lack of appropriate training. Moreover it is also observed that when officers from Non-IT background are placed at cybercrime branch, they need to undergo certain training, during that time they face problems in tackling these crimes.

Strategy:

Step 1: The officers that are placed in cybercrime cells must undergo a mandatory training before joining. These trainings can be conducted at IT / Cybercrime department at Police Training Academy or at CBI Academy. This training will help them in gaining knowledge about latest threats and how to tackle them. This training will reduce the wastage of efforts and time for training them at cybercrime branches and the existing officers can also function normally.

Step2: In terms of recruitment of police officers, there must be a quota for IT Professionals also. These officers must be specifically trained for cybercrime branches. Moreover, Transfer Policies for these trained officers must be changed and they must be transferred only in cybercrime branches and not to the normal police stations, since lots of efforts gets wasted to train them at some later stage.

5.6 MoU's with Educational Institutions

Scope: In order to combat the problem of lack of professionals and lack of appropriate software's, cybercrime monitoring agencies must collaborate with good institutions by introducing courses on cyber security in their curriculum and also focussing on software development for specific problems faced by investigation agency.

Strategy: In order to get better software more specific to our needs, cyber security agencies can conduct workshops on development of such software and at the end of which organize a competition for software development. Moreover incentivizing such activities can associate these students with these agencies for longer period of time.

Flowchart:

Fig 4: MoU's with Educational Institutions

5.7 Amendments in IT Act

Scope: In IT Act and its subsequent amendments, there exist some sections that need precise application, so that they cannot be misused. Moreover, many times due to these improper definitions, some innocent people also face imprisonment whereas criminals also get the chance to come out of jail in less time.

Strategy:

- **Cyber Terrorism (Sec. 66F):** Its scope must be limited down to cyber activities that create panic among large population or lead to mass destruction. Moreover, terms like decency / morality must be more precisely used with their proper application.
- **Child Pornography (Sec. 67B):** In this section, stress is laid on word child and that on the age below 18 years. In this section various forms of pornography must be included that may involve computer graphics involving children or adults imitating a child and making porn. Moreover, transmitting and viewing child pornography is a crime; similar conditions must also be put on adult pornography. A clause must be added in which ISP's must also be made responsible for any crimes committed by their network and they must be instructed to block / filter such contents.
- **Blocking Illicit Content (Sec. 69A):** This section must be strengthened to block any illicit content and this must be done by ISP's. In order to tackle the issues of internet censorship, specific guidelines for blocking of websites / content must be made. Moreover, a committee must be formed and they must analyse the parameters for such instructions to ISP's.
- **Mandatory Certification of E-Commerce Websites:** A section must be included that takes into account the security measures taken by E-Commerce websites and that must be insured by mandatory certification and rating these websites based on the level of security (This may be similar to star rating of electrical appliances).

5.8 **Forensic Labs Coordination**

Scope: Presently the forensic labs have a lack of professionals resulting in delay in investigation in many cybercrime cases. Moreover, due to lack of appropriate number of forensic labs, there is lack of coordination between various agencies. With the increase in cybercrime cases, there is a need to setup more forensic labs.

Strategy: Starting a pilot project by setting up a forensic lab at state level, that lab will cater to the cases of that state and associated agencies in that state. This may give us an insight into the coordination of these labs, viz., if there are sufficient experts or sufficient software is there or not. In the next level we can set up this model to many more states.

5.9 Contract with Websites Hosts

Scope: Majority of cybercrime cases investigation needs data / logs from website hosts. For majority of them, their servers are established in foreign countries. So in order to get information from these servers, we need to go through Interpol and most of the times information is not provided pertaining to privacy laws of that country.

Strategy: It must be made mandatory for website hosts to sign a contract asking them to cooperate in sharing of data, this can be either done by establishing servers in our country that will be governed by our privacy laws or by giving required data whenever needed, even if their servers are in some other country.

6. References

Articles / Reports / Laws:

1. IT Act, 2000 and IT (Amendment) Act, 2008
2. National Cyber Security Policy, July 2013
3. Crime in India, National Crime Records Bureau, Statistics for year 2012
4. Data Security Council of India (DSCI) (http://www.dsci.in/)
5. Indian penal Code (IPC) for basic crimes that also fall in domain of IT Act
6. Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL)
7. European Convention on Cybercrime
8. United Nations Office on Drugs and Crime (UNODC) Comprehensive Study on Cybercrime, Draft, February, 2013
9. Justice S. B. Sinha, "*Cyber Crime in the Information Age*", Cyber Space and The Law – Issues and Challenges, NALSAR University, 2004
10. Cyber Crime and its Jurisdiction in India, by Abhay Pratap Singh and Pranay Bagdi
11. UNCITRAL and European Convention on Cybercrime
12. Comprehensive Study on Cybercrime, UNODC, 2013
13. Sophos Security threat Report 2013 (http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx)
14. Fortinet 2013 Cybercrime Report
15. 2012 Norton Study: Consumer Cybercrime estimated at $110 Billion Anually (http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02)
16. 2012 Cost of Cybercrime Study: United States, by Ponemon Institute
17. RSA 2012 Cybercrime Trends Report
18. Short Note on IT Amendment Act, Pranesh Prakash, http://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008
19. Information Security Awareness CDAC, http://www.infosecawareness.in/

20. CERT-In Website, http://www.cert-in.org.in/
21. http://www.first.org/resources/guides
22. Satheesh G Nair's Blog on Cybercrime, For case studies, http://satheeshgnair.blogspot.in/
23. Cyber Law Consulting, for case studies, http://www.cyberlawconsulting.com/cyber-cases.html
24. Present trends of Cybercrime, http://www.go-gulf.com/blog/cyber-crime/

Newspaper or Magazine Articles:

25. N Vidyasagar. "India's Secret Army of Online Clickers" The Times of India (May 3, 2004)(http://timesofindia.indiatimes.com/business/india-business/Indias-secret-army-of-online-ad-clickers/articleshow/654822.cms)
26. An IT superpower, India has just 556 cyber security experts (http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece)
27. Govt approves National Cyber Security Policy (http://www.thehindubusinessline.com/government-and-policy/govt-approves-national-cyber-security-policy/article4696051.ece)
28. Implementing National Cyber Security Policy is a challenge: Sibal (http://www.firstpost.com/india/implementing-national-cyber-security-policy-is-a-challenge-sibal-921427.html?utm_source=top_menu)
29. CCTV footage from Delhi metro stations land on porn websites: reports (http://www.ndtv.com/article/cities/cctv-footage-from-delhi-metro-stations-land-on-porn-websites-reports-389932)
30. Cyber-crime complaints shoot up in Bengal (http://timesofindia.indiatimes.com/city/kolkata/Cyber-crime-complaints-shoot-up-in-Bengal/articleshow/20672053.cms?intenttarget=no)
31. Delhi Police launches cyber awareness campaign (http://articles.timesofindia.indiatimes.com/2013-02-20/internet/37199132_1_cyber-crime-cyber-laws-internet-safety)

32. Delhi Police to teach teens social network ethics (http://articles.timesofindia.indiatimes.com/2013-02-20/social-media/37199001_1_cyber-laws-awareness-programme-cyber-cell)
33. Govt goes after porn, makes ISPs ban sites (http://timesofindia.indiatimes.com/tech/tech-news/internet/Govt-goes-after-porn-makes-ISPs-ban-sites/articleshow/20769326.cms?intenttarget=no)
34. Man lured by honey trap on Facebook, killed (http://timesofindia.indiatimes.com/%20http://timesofindia.indiatimes.com/city/chennai/Man-lured-by-honey-trap-on-Facebook-killed/articleshow/20771965.cms?intenttarget=no)
35. US gathered citizens's internet records under PRISM (http://timesofindia.indiatimes.com/tech/tech-news/internet/US-gathered-citizenss-internet-records-under-PRISM/articleshow/20812153.cms?intenttarget=no)

7. APPENDIX

7.1 Mentor Meetings

1st Meeting

Date: May 18th 2013

Time: 3:00 PM

Duration of Discussion: 1 hour 25 minutes

Discussion:

- How to develop a research methodology regarding the topic
- Setting up of agenda for the project and discussion on framework of report
    - Problem Description (Motives, types of cyber criminals and effect and consequences of cyber-attacks)
    - Literature analysis / Document study (Comparison of Foreign Domestic Laws and International Laws)
    - Case studies and surveys
    - Jurisdictional issues
    - Recommendations for changes in laws
    - Good practices guidelines
- Classification of cyber-crime (on basis of motives)
    - Economic
    - Personal: Causing Reputational Harm, Mental and Physical Harassment
    - Ideological: To create panic and fear among general public (cyber terrorism)
- Discussion on domestic laws that are made by a country and international laws. Aim of discussion was to get knowledge on recommendation writing

Action Items before next discussion:

- Preparation of a Plan of Action to cover the whole agenda
- Development of basic idea of cybercrime through intensive study via internet

- Study of Indian laws and their implications (Aim will be to study all the possible ways in which Indian government can take action in any case of cybercrime)
- Analysis of Foreign Domestic Laws of other countries and comparing them with ours

References:

- Literature Analysis / Document Study
    - Information Technology Act, 2000
    - Information Technology (Amendment) Act, 2008
    - Data Security Council of India (DSCI)
    - Indian Penal Code (for cheating)
    - Council of Europe Convention on Cyber Crime.
    - UN Citral Model on E-Commerce
    - UNODC (United Nations Office on Drugs and Crime) on Cyber Crime
- Persons to meet after next week
    - Mr. Sebastian, General Manager, GMR
    - Mr. Triveni Singh, Add. SP, UP Police
    - Mr. Sanjay Gautam, Inspector, CBI
    - Mr. Babu, CERT-in

2nd Meeting

Date: June 3rd 2013

Time: 6:00 PM

Duration of Discussion: 30 minutes

Discussion:

- Discussion regarding some cybercrime case studies done by me on some cybercrimes in India. (Source of case studies was internet)
- Checking authenticity of the case studies available on internet from data available on National Crime Records Bureau (NCRB)

- Discussion on Jurisdictional issues as mentioned in European Convention on Cybercrime

Action Items before Next Discussion

- Meeting Mr. Sanjay Gautam, Inspector, CBI Academy (expert on computer and cyber forensics)
- Getting authentic details about cybercrime case studies found on internet
- Refined study of UNCITRAL and European Convention on Cybercrime

References:

- Mr. Sanjay Gautam, Inspector, CBI Academy, Ghaziabad
- Mr. Triveni Singh, SP, UP Police (Expert in Cybercrime and Financial Fraud)
- Mr. Babu at CERT-In
- Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law
- European Convention on Cybercrime

3rd Meeting

Date: June 18th 2013

Time: 3:30 PM

Duration of Discussion: 1 hour

Discussion

- Analysis of Cybercrime Statistics to be done from Crime in India report by National Crime Records Bureau for 2012
- For recommendation regarding awareness generation, discussed, what are parameters of awareness, viz., Precautions by users and Identifying threats and vulnerabilities.
- The focus for awareness generation will be
    - What tools one should use to secure his/ her PC or network

  - What good Practices Guidelines one should follow to prevent damage due to cyber-attack.
- **Model for Awareness Generation:**
  - **How much Damage:** Telling the people case studies and the amount of damage that took place. This is done to have an impact on people‟s mind to take some action for their cyber security
  - **What to do:** Telling people about various places where they can go to seek help in case of any cyber-attack and what actions they can take themselves to sort the issue.
  - **Knowledge Providing:** This includes dissemination of information and good practice guidelines at various levels like higher educational institutions, school teachers, children and parents.
  - **How to Propagate:** This step focuses on propagation of this information among various communities active on internet. Using case studies can be important tool to propagate some message. This can be done using various means like social networking, print media coverage, inclusion in books of schools, workshops and lectures.

- **Recommendation for E-commerce:**
  - Accreditation of every website involved in online transactions.
  - Standard Security Audit must be there for all websites.
  - This Cyber Security Audit should be done by professionals trained and certified by government.
  - There must be a system in which we must rate websites on the basis of their security measures taken to secure the credentials of their customers.
- Blocking of Harmful or obscene websites must be done, government is entitled to do so if they pose any harm to our country.

Action Items before Next Discussion

- Reading of Crime in India report by National Crime Records Bureau for 2012.

References (People to meet, research report or papers to read)

- Meeting with Shri S D Mishra, Addl. DCP, Economic Offences Wing, Delhi Police.
- Meeting with Shri Triveni Singh, SP, UP Police.

7.2 Field Visits

1st Field Visit

Date: June 4th 2013

Institution: CBI Academy, Ghaziabad

Name: Mr Sanjay Gautam

Designation: Inspector, Faculty (Computer and Cyber Forensics)

Topic of Discussion:

1. **Awareness among users:** A major step towards prevention of cybercrime. Agencies must be set up to spread awareness among public, keeping check on cyber café and issuing warnings to people who are getting involved in such crimes.
2. **Unsecure networks falling prey:** In India it has been seen that many government offices and universities use open proxies and does not have any security measure taken to prevent its unauthorized use. Due to this reason these IP addresses are used by unauthorised people (even by Cybercriminals) for wrong uses.
3. **Lack of International ties:** India does not have a mutual agreement related to cybercrime with countries and as a result of this, if we want to get any data, we are unable to get it since most of these company's servers are in other countries.
4. **Presence of Harmful Websites:** There are many websites which uses open proxies, shows obscene material and can be used to send anonymous mails. It is even harder to get data from these websites hosted in other countries, during investigation of cases. Government

should take strict measures to identify and block these websites in our country. Steps must be also taken to prevent all the virtual money transactions going in cyberspace, as it is violation of FARA.

5. **Increasing efficiency of CERT-In:** Steps must be taken to make CERT-In more active, this can be done by establishing nodal offices of CERT-In at state level, new recruitment for trained professionals must take place and each nodal centre must be responsible for solving regional issues and spread awareness among public, also about the misuse of their network by other people. This must be done by organizing seminars and workshops at educational institutes.
6. **Lack of Professionals:** The present situation with Indian investigation agencies is that there are few trained professionals to combat cybercrime. Officers at higher posts (decision making positions; even in-charge of cybercrime branches) also lack necessary skills needed to tackle cybercrimes, due to this these branches does not work efficiently. It is needed to bring professional lot of people in investigation teams or there must a training program for even lowest level officer.
7. **Lack of knowledge at Sub- Inspector level:** Sub-Inspector is the first person who responds to the complaints of people. But according to Sec. 80 of IT Act, 2000, Inspector is the lowest level of officer that will deal with issues of cybercrime and majority of inspectors and sub-inspectors don't have adequate knowledge in cybercrime, as a result of this very few cases of cybercrime gets registered. Steps must be taken to train inspectors about cybercrimes and IT Act's provisions. Even after registering cases the defence lawyer has upper stand since police officers lack proper knowledge regarding cybercrime and their legal provisions.
8. **Hierarchy in Police stations:** In the present scenario, even trained professionals have no incentives to work in government agencies since there is lot of hierarchy order in offices and in most situations higher post officers are not professional, so the work done by lower officers gets inadequate response, thus leading to demotivation.

9. **Power to Police:** In order to track tentative criminals and prevent subsequent crimes, police must be empowered, for eg. in order to catch criminals involved in sending obscene materials, police must be allowed to make fake social networking profiles and subsequently catching the criminals. Moreover, there must follow-up sessions for such criminals to tell the police station about their whereabouts after completion of sentence, also police can keep an eye on them.
10. **Improper definitions in Laws:** Laws related to Cyber terrorism, Pornography, Cyber café guidelines and offensive messages is unclear and can be misused to harm for some vested interests.
11. **Lack of software development centres in India:** In cyber forensics, some software with specific features are required and in the present scenario our government is buying these software from foreign countries that are made for their specific need, so sometimes it also goes ineffective in investigation of some cases. Government must collaborate with technical institutions in our country to develop software by taking feedback from investigation agencies. This will not only lead to effectiveness in investigation but also in reduction of expenditure.

2nd Field Visit

Date: June 8th 2013

Institution: CERT-In (Indian Cyber Emergency Response Team)

Name: Mr Omveer Singh and Mr S Babu

Designation: Scientist, CERT-In

Topic of Discussion:

1. **Awareness among users:** Public is unaware of basic security measures that need to be followed, they don't have antiviruses, uses pirated software.
2. **Inaccurate working of officials:** Not doing their work proactively, no proper training, greedy nature, transfer policy.

3. **No initiatives from educational institutes:** At present majority of colleges don't have courses in cyber security nor they take steps to generate awareness among students.
4. **Cyber Auditing:** Lack of cyber auditors and no steps taken by CERT-In as well as police to do cyber audits.
5. **Specialized cybercrime teams:** No teams at present to look into local cybercrime issues. Specialized officers for cyber cells not present.

Action Planned:

6 To look for better methods to generate awareness. Some websites work in this field.

7 To look forward into the issues faced by cyber professionals and find solutions

8 Good practices guidelines must be publicized and enforced in educational institutions.

9 Steps must be taken to conduct cyber audit and incentivize training of cyber auditors.

10 CERT-In nodal branches must be set up and senior officers in cyber cells must be proficient in cyber security issues.

3rd Field Visit

Workshop on Cyber Crime Investigation and Cyber Forensics, CERT-In

Date: 14th June 2013

Speakers: Sh. Omveer Singh, Addl. Director, CERT-In

Sh. S Babu, Scientist, CERT-In

Topic of Discussion:

1. Cybercrime and Cyber Forensics: An Overview
2. Role of First Responder and Seizing of digital evidence in various cybercrime scenarios
3. Imaging and Integrity verification of Digital Evidence

4. Best Practices of collecting digital evidence
5. Analysis of digital evidences

Key points of Discussion:

- Types of Vulnerabilities:
    1. Unpatched Vulnerability
    2. Zero Vulnerability
    3. Induced Vulnerability
    4. Non- Vulnerability
- Due to unsecured networks, cybercriminals can scan the network and easily target the vulnerable systems, they gets information like
    1. Alive computer/ hosts
    2. Operating systems
    3. Configuration of machine
    4. Filtering and secondary systems
- Common methods used by cybercriminals:
    1. Social Engineering
    2. Email Spoofing/ Spamming
    3. Scan/ Probes
    4. Bot-nets
    5. Cyber Frauds
    6. Counterfeiting of Documents
- Type of Frauds:
    1. Auction Fraud
    2. Investment Fraud
    3. Clicks Fraud
    4. Charity Funds
    5. Payment Card Credentials
    6. Advanced Fee Fraud(Nigeria 419 Fraud)
- Computer system Compromise:
    1. Access, modification and misuse of confidential data
    2. Cyber terrorism

3. Organized crimes/ gangs
4. Encrypting vital documents

- Social Engineering: Phishing & Vishing(Phishing on voice call)
    1. Malware by emails
    2. Drives in by download
    3. I-Frame injection
    4. Botnet installation
- Malwares: Self- executing & replicates by executing itself. It does the task that normal program must not do.
    1. Worm
    2. Trojan Horse
    3. Keyloggers
    4. Autorun malware
- Possible solutions to frauds:
    1. Biometric Transactions
    2. Security Audit
    3. Intrusion Prevention System
- DoS/ DDoS: Denial of Service / Distributed Denial of Service
    1. Block IP address sending useless mails.
    2. Use of large bandwidth by websites having load by genuine users.
- Digital Evidence collection:
    1. Ram Dump and getting image of ram in external hard disk.
    2. After crime, do not shut down computer, disconnect internet.
    3. Latent data and extremely fragile
- Cyber Forensic Investigation Process
    1. Log Analysis
    2. Identification
    3. Seizure/ Acquisition
    4. Imaging and Integrity verification
    5. Tracking IP of cybercriminal
    6. Analysis and Documentation

4th Field Visit

Date: June 26th 2013

Institution: Economic Offences Wing(EOW), Delhi Police

Name: Mr. Vijay Gehlawat

Designation: Inspector, Cybercrime Branch, EOW

Discussion:

- Government websites hosted by NIC are secured enough and never faces security breach, even if any intrusion takes place it is from the client end not from NIC end.
- For Internet Banking, almost all cybercrimes are due to credential theft and very minimum of them takes place due to fake pages.
- Financial scams (like Nigeria 419 scam) takes place at three levels, level1 are the master minds back in Nigeria making all the web based services, Level 2 are India based people (hired by Level 1 persons), Level 3 are the fake SIM's that are used by Level 2 to commit these crimes.
- Regarding open proxies used by some government institutions, it is also sometimes intentionally kept open in order to get hold of cyber criminals using these mediums.
- In IT Act, many penal provisions are for varying cybercrimes and all of them are bailable. There is no distinction mechanism between innocent person and the criminal. As a result of this innocent person has to be in jail whereas original criminal also gets bail and can easily commit other crimes.
- Monitoring of ISP's is a necessary, at present ISP's show very casual behaviour towards cyber security. ISP's are not worried since they are not held responsible along with the culprit.
    - No filtering of data is done by ISP's
    - No strict check is kept on ssle of SIM cards

- There is a need of more specialized teams handling cybercrimes specially trained to handle these crimes and also guide other institutions to handle such crimes.
- Forensic labs (FSL's) coordination is very less at present because they have lack of professionals to conduct evidence investigation, as a result of this cases pile up a lot.

References:

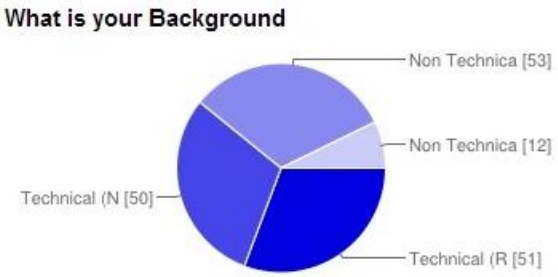
- Bureau of Police Research and Development, R K Puram, Delhi
- NCRB, IT Police Station

7.3 Surveys

Survey conducted over students from different backgrounds regarding Basic Cyber Security Awareness. A total of 179 responses were recorded. Aim of this survey is to get information regarding

- Most frequently visited places on internet,
- Knowledge regarding threats on internet,
- Knowledge regarding vulnerable systems,
- Awareness about government efforts to secure Indian citizens from cyber-attacks,
- Possible ways to generate awareness

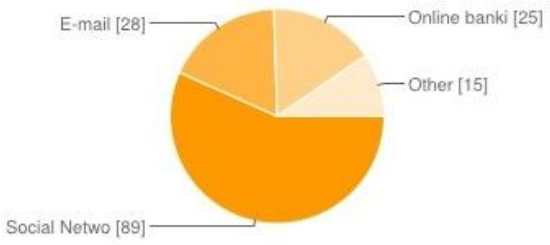
Results:



Technical (Related to computers)	51	31%
Technical (Not Related to Computers)	50	30%
Non Technical (Up to general use of computer)	53	32%
Non Technical (No knowledge of computers)	12	7%

Survey was conducted among students of many colleges, including technical as well as non-technical background. Getting responses by students from diverse background helped in understanding the overall scenario of the awareness among youth of country.

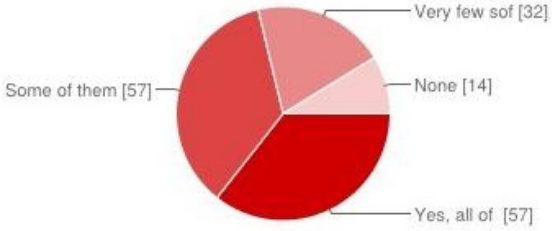
Which places you spend most of your time on internet



Social Networking Sites	89	57%
E-mail	28	18%
Online banking / Shopping / Ticket Booking	25	16%
Other	15	10%

Majority of users on internet go for Social Networking sites or for Emails. Moreover, majority of cybercrimes takes place through these mediums only. So these places can be targeted to spread awareness among users.

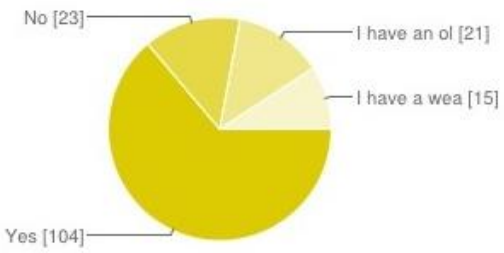
Do you have genuine software on your PC



Yes, all of them	57	36%
Some of them are pirated(about 30% or less)	57	36%
Very few software are genuine	32	20%
None	14	9%

It was observed that 60-70% of users don't have genuine software, during awareness generation; emphasis must be laid on importance of genuine software.

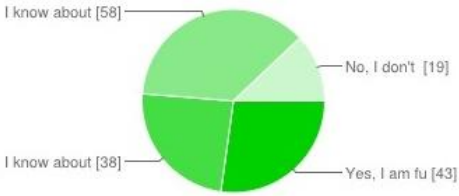
Do you have genuine antivirus software installed on your computer



Yes	104	64%
No	23	14%
I have an old one (does not gets updated)	21	13%
I have a weak antivirus	15	9%

Antivirus software is the basic necessity to protect your system from threats on internet

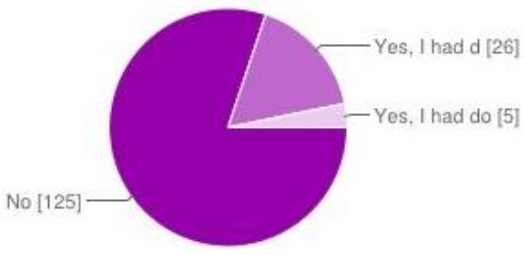
Do you know about existing threats on internet and what are their sources



Yes, I am fully aware of these threats	43	27%
I know about many of them and also have knowledge about their sources	38	24%
I know about some of them but unknown to many of them	58	37%
No, I don't know anything about these threats	19	12%

Awareness campaign must also focus on 'Whom to Approach', if there is a cyber-attack. By this they will come to know about government agencies / policies in this regard.

Have you ever disclosed confidential details on internet or have responded to some phishing mail

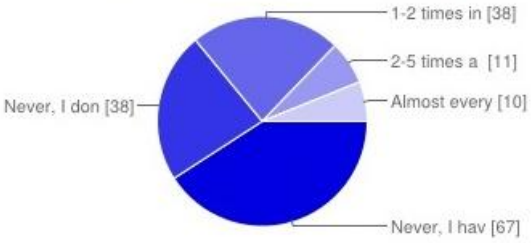


No	125	80%
Yes, I had done that few times	26	17%
Yes, I had done this many times	5	3%

Majority of financial cybercrimes takes place due to disclosure of confidential details by public itself, this is mainly done through phishing mails accompanied with

offers of windfall gains and lotteries to lure them.Since 90% of financial cybercrimes takes place through credential theft by using phishing mails / fake pages. Guidelines must be spread to avoid such thefts.

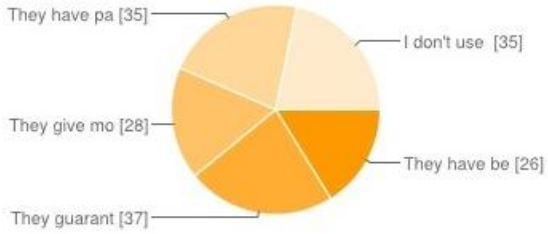
How often do you see virus / malware / spyware on your computer



Never, I have very strong Antivirus	67	41%
Never, I don't have strong Antivirus	38	23%
1-2 times in a week	38	23%
2-5 times a week	11	7%
Almost everyday	10	6%

This also gives an insight into the level of vulnerable system used by public.

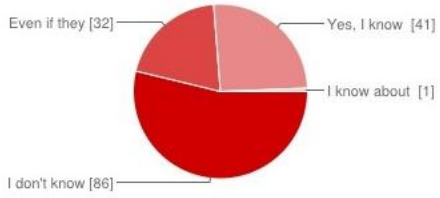
Do you prefer some online shopping sites over another, it is because



They have better security for credentials of customers	26	16%
They guarantee of sending Genuine product	37	23%
They give more discount / coupons	28	17%
They have payment on delivery option	35	22%
I don't use online shopping websites	35	22%

E-Commerce websites must be made safe to avoid credential theft of customers.

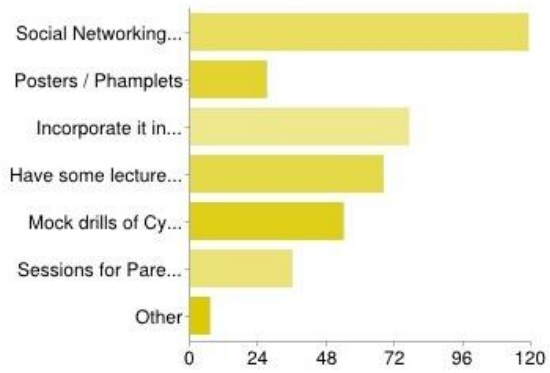
Do you know about any initiative taken by government to prevent Indian citizens from cyber attacks.



I don't know	86	54%
Even if they provide any protection, I don't believe they are secured enough	32	20%
Yes, I know little bit about some cyber support agencies, like, CERT-In, CDAC, etc.	41	26%
I know about these websites and I am subscribed to their mailing lists	1	1%

Government efforts also needs proper marketing and publicity to reach its audience.

If someone wants to spread awareness about cyber security and threats, what will be the best way to do that.



Social Networking Websites	119	31%
Posters / Phamplets	27	7%
Incorporate it in School Education	77	20%
Have some lectures / Seminars for college students	68	18%
Mock drills of Cyber attacks by government agencies	54	14%
Sessions for Parents and Teachers	36	9%
Other	7	2%

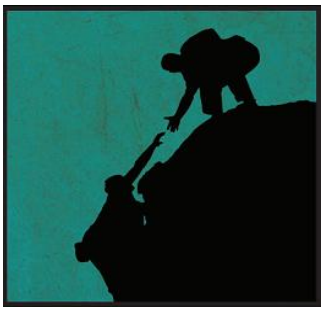
These are some of the mechanisms that can be adopted to generate awareness among public.

"The highest measure of democracy is neither the 'extent of freedom' nor the 'extent of equality' but rather the highest measure of participation."
- A.D. Benoist

Rakshak Foundation creates awareness domestically and internationally about the rights and responsibilities of citizens towards the society and state. Rakshak engages in and supports social and scientific research on public policy and social issues.

GET INSPIRED

IDENTIFY YOUR PASSION



GET INVOLVED

Contact:

Email: secretary@rakshakfoundation.org
Website: www.rakshakfoundation.org

Disclaimer: This report is an outcome of a student project and the content of this report represents the views of its author. Neither the report nor any of its parts represent the views of Rakshak Foundation and/or any of its affiliates and officials in any capacity whatsoever. The figures and facts used in the report are only suggestive and cannot be used to initiate any legal proceedings against any person or organization. However, the author shall be extremely grateful to acknowledge any inaccuracies in the report brought to author's notice.
Please email your suggestions or concerns to: hr@rakshakfoundation.org]