STUDY OF FACTORS AFFECTING EFFECTIVE INVESTIGATION OF CYBER CRIMES IN PUNE REGION

A Thesis

SUBMITTED TO THE
TILAK MAHARASHTRA VIDYAPEETH, PUNE

FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY (Ph.D.)
In MANAGEMENT Subject

Under the Board of POST GRADUATE Studies

BY

SWATI NITIN SAYANKAR
(Registration No. 15813007828)

UNDER THE GUIDANCE OF
DR. PROF. ASHA NAGENDRA

DEPARTMENT OF MANAGEMENT

June 2018

FORM 'A'

Study Of Factors Affecting Effective Investigation of Cyber Crimes In Pune Region

A Thesis submitted to

Tilak Maharashtra Vidyapeeth, Pune

For the Degree of Philosophy (Ph.D.)

Subject: Study Of Factors Affecting Effective Investigation of Cyber Crimes In Pune Region

Under the Board of POST GRADUATE Studies

Name of the Candidate : Swati Nitin Sayankar

Under the Guidance of : Dr. Prof. Asha Nagendra

Name of the Department : Management

Month and Year : June 2018

FORM 'B'

I hereby declare that the thesis entitled **"Study Of Factors Affecting Effective Investigation of Cyber Crimes In Pune Region"** completed and written by me has not previously been formed as the basis for the award of any Degree or other similar title upon me of this or any other Vidyapeeth or examining body.

Sd-

Swati Nitin Sayankar
Signature of the Research Student

Place : Pune

Date : June 2018

FORM ‘C’

CERTIFICATE

This is to certify that the thesis entitled **“STUDY OF FACTORS AFFECTING EFFECTIVE INVESTIGATION OF CYBER CRIMES IN PUNE REGION”** which is being submitted herewith for the award of the Degree of Vidyavachaspati (Ph.D.) in Management Department of Tilak Maharashtra Vidyapeeth , Pune is the result of original research work completed by Mrs. Swati Nitin Sayankar under my supervision and guidance. To the best of my knowledge and belief the work incorporated in this thesis has not formed the basis for the award of any Degree or similar title of this or any other University or examining body upon him / her.

Sd-

Dr. Asha Nagendra
Signature of the Research Guide

Place: Pune

Date: June 2018

ACKNOWLEDGEMENT

My special thanks goes to my guide respected Dr. Asha Nagendra whose research perspective and guidance helped me in completion of Ph.D. work. Her motivation helped me to complete the thesis.

My thanks to Mr. Sandeep Gadia (Cyber consultant, India Cyber lab, Pune) who was throughout cooperative starting from choosing the topic to completion of thesis. Thesis moved with his support. He shared his valuable time, knowledge, expertise in the field which gave me insight of the selected topic.

I am also thankful to Mr. Rajas Pingale, Cyber Law Consultant (Pune) who explained me the legal prosecution of cyber crimes and legal challenges during its investigation.

I am thankful to Mr. Deepak Sakore, Deputy Commissioner of Police **(EOW & Cyber Cell) Crime** for his valuable guidance extended Co-operation, Support and also thankful to Sr. Police Inspector Mr. Sunil Pawar, Cyber Crime Cell, Pune who gave me timely information related to cyber crime investigation process and his Co-operation for providing the required information time to time.

I am very much thankful to all other Assistant Commissioner of Police of all the divisions police stations of Pune city as well as authorities / officers from Cyber Crime Investigation Cell (Pune, Mumbai, Thane),Cyber Forensic laboratories (Santacruz, Mumbai) for furnishing information on time on cyber crimes required for this research work. Their experience, interactions and information helped me in fulfilling the objective of this research project.

Last but not the least I am grateful to my Parents and my Children for their constant support throughout the completion of thesis.

TILAK MAHARASHTA VIDYAPEETH

UNDERTAKING

1. I SWATI NITIN SAYANKAR, have registered my name for the Ph.D. course in MANAGEMENT in the year 2013-14 with PRN No. – 15813007828
2. The undertaken research is entitled as :

   TITLE : "STUDY OF FACTORS AFFE -+*CTING EFFECTIVE INVESTIGATION OF CYBER CRIMES IN PUNE REGION"
3. I have gone through extensive review of literature of the related published/unpublished research works and the use of such references made has been acknowledged in my thesis.
4. The title and the content of research is original.
5. I understand that, in case of any complaint especially plagiarism, regarding my Ph.D. research degree will be withdrawn from any party, I have to go through the enquiry procedure as decided by the Vidyapeeth at any point of time.
6. I understand that, if my Ph.D. thesis (or part of it) is found duplicate at any point of time, my research degree will be withdrawn and in such circumstances, I will be solely responsible and liable for any consequences arises thereby. I will not hold the TMV, Pune responsible and liable in my case.

I have signed the above undertaking after reading carefully and knowing all the aspects therein.

Signature

Address: "SHREE NANDAN" ,A-19, LANE 7, SHAHU COLONY, NEAR CUMMINS COLLEGE, KARVE NAGAR, PUNE -411052, MAHARAHSTRA

Phone No. : +91 9822091969 E-mail : swatisayankar@rediffmail.com

Date : June 2018 Place : PUNE

Table of Contents

List of Tables

List of Figures

List of Appendices

CHAPTER 1 - INTRODUCTION

This Chapter is discussed under following heads

1.1 Computers and Internet in 20th Century

1.2 Introduction to cyber crime

- Cyber Security
- Cyber-attacks and its effects
- Scope of Cyber crime
- The motives behind cyber crime
- Cyber Criminal
- Profile of cyber criminals
- Characteristics of cyber crime
- Reasons for cyber crime
- Unique features of cyber crime
- Classification of cyber crimes
- Target Segments of cyber crimes
- Scope of Cyber Laws in India
- Laws applicable to cyber crimes

1.3 Study of reports on cyber crime

1.4 Motivation for research

1.5 Need of research

1.6 Social Relevance of Research

1.7 Objectives of the Research

1.1 COMPUTERS AND INTERNET IN 20TH CENTURY

In 20th Century, new technologies have started emerging for betterment of mankind and along with this its use also started increasing. The invention of computer is the most noteworthy achievement of all the significant achievements made by the mankind,. The emergence of computer networking provided an excellent method of transmission of information across the world the result of which the world has now virtually become global village.

Internet attracted mass and in short time span, technology of Internet has crossed all geographical barriers & captured mind and heart of every Citizen being called 'Netizen' later due to its tremendous use. Communication has increased across countries for sharing knowledge, views and feelings using Internet.

Internet proved extremely beneficial on one side. On another side due to its security and privacy problems, its misuse had been started which gave rise to new crimes in society known as 'Cyber crimes'.

With view to countering Internet and Computer related crimes, the Indian Parliament approved a new legislation, namely the Information Technology Act, 2000 to tackle problems related to IT i.e. Information Technology. The act came into force on October 17, 2000. It deals with various cybercrimes related to internet and cyberspace, particularly unauthorized access, virus attacks, denial of access, or any contaminant causing damage to computer software etc.

1.2 INTRODUCTION TO CYBER CRIME:

Cyber crime consists of all the activities related to crime and these activities are done using the means of communication devices like computers, cell phones, tablets, internet, worldwide web, cyber space.

Any activity that uses computer as a tool, target or a means for executing crime falls within the scope of cyber crime. The Indian Law- The IT Act, 2000 has not defined the term 'cyber crime'.

The term ‘cyber crime’ is not included in IPC (Indian Penal Code). It does not use it anywhere though the IT Act, 2000 is amended by IT (Amendment) Act 2008- the Indian Cyber Law. However, ‘Cyber Security’ is defined under the section [2-nb]. It means safeguarding data, information, Computer peripherals, communication devices and information stored in it from unauthorized, illegal access, its misuse, disclosure, editing or destruction.

In the Indian context, cyber crime is punishable under the IT ACT 2000. Cyber crimes are considered under Penal consequences under the IPC or Indian Penal Code.
According to IT Act 2000, Cyber Crime can be defined as a “voluntary and willful act” that badly affects an individual or valuables or an individual’s computer systems. The IT Act, 2000 is amended by Information Technology (Amendment) Act, 2008. This is well known as the ‘Cyber law’. This Act has special Chapter-11 titled as “Offences”. In this chapter, various cyber-crimes have been declared. They are known as penal offences. All these penal offences are punishable. Punishment includes imprisonment and fine to an individual for committing cyber crime.

Cyber crimes can be discussed under the following headings.

- **Cyber Security**
- **Cyber-Attacks And Its Effects**
- **Scope Of Cyber Crime**
- **The Motives Behind Cyber Crime**
- **Cyber Criminal**
- **Profile Of Cyber Criminal**
- **Characteristics Of Cyber Crime**
- **Reasons For Cyber Crime**
- **Unique Features Of Cyber Crime**
- **Types /Classification Of Cyber Crimes**
- **Target Segments Of Cyber Crimes**
- **Scope Of Cyber Laws In India**
- **Laws Applicable To Cyber Crimes**

- **CYBER SECURITY**

The term “Cyber Security” refers to three main things·

1. It is a group or set of activities which may be technical and non-technical,
2. It is meant to safeguard computers and computer related networks, hardware and software. It also safeguards the information of all these assets or devices they contain. It protects software and data, as well as other elements of cyberspace. It protects it from all damages or threats. Damage or Threats may include all threats to the national security.
3. It refers to the extent of protection as a result of applications of these activities and measures.

The related field of information security consists of dedicated, systematic efforts such as analysis of research data aimed at implementing the activities that improves the overall quality of security.

- **CYBER ATTACKS AND ITS EFFECTS**

Cyber space is constantly under danger physical attack or assaults. Cyber thieves, hackers break into Computer systems, steal personal data and confidential secrets, hack websites, disturb services, destruct data and network systems. They spread computer viruses and worms by conducting misguiding transactions. The aim is the harassment of individuals annoying them and organizations.

Cyber attackers are wise enough to scan military operations. They can disturb or break target’s communications, command and control. They can influence governments, events, organizations, persons. By way of cyber espionage, important information and national, state secrets can be obtained by these cyber attackers.

- **SCOPE OF CYBER CRIME**

Cyber crimes are growing rapidly. It is an increasing phenomenon. This is happening not only in India but all over the world. Its speed is directly related to the level of progress made in Computer Technology by every country. This is realized to be an area of serious concern not only for other countries but also India.

The cyber terrorists made attack on India's Parliament on 13th December, 2001. This is an example that how computer networks are being misused by the anti-nationals.

- **THE MOTIVES BEHIND CYBER CRIMES**

According to NCRB in 2014, 9622 cases of cyber crimes were registered. Cyber crimes are committed with following motives. NCRB has identified various motives behind cyber crimes.

Table 1: Motives behind Cyber crimes

Motive	Cases
Greed /Financial gain	1736
Insult to modesty of women	599
Fraud / Illegal gain	495
Sexual exploitation	357
Personal Revenge	285
Causing disrepute	272
Extortion	199
Inciting hate crime against community	174
Motives of Blackmailing	159
Emotional motives like anger, revenge	139
Prank/Satisfaction of gaining control for developing own business invest	110
Political motives	75
For spreading privacy	52
Sale/ purchase of illegal drugs	27
Disrepute public services	25
Inciting hate crimes against country	11
Steal information for espionage	3

From above list of different motives, Greed/financial gain was the leading motive for cyber crime. 'Insult to modesty of women' and 'Sexual exploitation' were amongst the top 5 motives.

- **CYBER CRIMINAL**

Cyber criminals are involved in criminal activities. Criminal activities include electronic fraud, child pornography, software piracy, unauthorized access to computers, cyber stalking etc. These crimes are done using their skill and knowledge in Information or computer technology. We can say that cyber criminals are highly knowledgeable hi-tech people. They invade rights of computer owners/users by unauthorized access to their computer system or computer networks.

Cyber criminals may constitute various groups or organizations according to objective of their criminal activities. Other category of cyber criminals may be as follows.

1) Children and teenagers between the age group of 8 to 18 years
2) Professional Hackers
3) Disgruntled/ unsatisfied employees

- **PROFILE OF CYBER CRIMINALS**

The cyber crimes committed by cyber criminals have different ‘Profile’.

Table 2: Profile of cyber criminal arrested in 2014

Profile	**Arrests**
Neighbors / Relative	427
Student	320
Professional Computer Hacker/Cracker	207
Employee/Disgruntled employee	191
Sexual Freak	163
Business Competitor	149
Religious person	77
Political person	29
Persons with Psychological disorder	23
Foreign National	8
Cyber Terrorist	1

As per report studied of NCRB from 2011-2015, Cyber criminals are generally from the age group of 18-30 years are more than age group of 30 years and above.

- **CHARACTERISTICS OF CYBER CRIME**

Characteristics of Cyber crimes are totally different from that of a traditional crime. The most important features of cyber crimes is that they are white collar crimes. They are easy to commit compared to other crimes, hard to find or detect and harder to prove. Cyber criminals with fundamental computer knowledge with little expertise and skill can easily destroy valuable database causing heavy loss or damage to the affected victim of the crime.

Evidences against the cyber crime are easy to erase. The computer or computer network used for the information capturing has the feature of impersonality or anonymity and openness. This is easy for cyber criminal to involve in crime and not being identified. This gives them liberty to commit more and more crimes.

- **REASONS FOR CYBER CRIMES**

Any criminal activity that is considered as crime comes under IPC (Indian Penal Code).When it makes use of a computer is then treated as a cyber crime. The computer can be used as a medium or target to commit a crime.

The computer systems though of higher technologies, its devices are extremely vulnerable to cyber attacks. This technology can be easily misused to exploit a person or his computer system or organization’s network by illegal means or unauthorized access.

Innocent computer users become victim of cyber crimes due to lack of knowledge to protect and safeguard their computers. Cyber crimes happen due to vulnerability of computers. The reasons of being attacked or Vulnerabilities to cyber criminality may be elaborated further as follows:

1. Enormous Data.
2. Wider access to information
3. Negligence of network users
4. Public Wi-Fi Threats
5. Loss or Non availability of evidence
6. Accessibility to victim
7. Jurisdictional uncertainty

1. Enormous Data

Criminals can access Computers data of various fields. They get the privilege to access large amount of data and this data can be erased, replaced or deleted through various methods, including virtual or physical.

2. Wider access to information

Confidential or private and secret data is stored online or on networks. This includes data of security agencies, scientific data / information / secrets, financial institutes and even governmental organizations. This motivates cyber criminals to take disadvantage of unauthorized access to data and use it for own motives or against nation. Complicated technologies can be changed. Firewalls may be compromised, permitting cyber criminals to get access to security code words, bank account holder's details and other confidential information.

3. Negligence of network users

Sometimes simple carelessness or ignorance can give rise to crimes e.g. saving or storing a password on an office computer, using official data in a place which public uses and even storing data without assigning password etc. The cyber criminal can take disadvantage of such ignorance or negligence on user's part. He can make use of it to gain, change or create information.

4. Public Wi-Fi Threats

Public Wi-Fi may seem like one of the greatest conveniences, but in reality, it can be quite dangerous. While public Wi-Fi has its benefits, it's convenient and in most cases free it also comes with drawbacks, including its security risks.

Free public Wi-Fi is a concern because when you connect to free Wi-Fi, it's generally unencrypted. That means anyone can see what you're up to over the network. They can see what sites you're visiting and what you're typing into them. Even if you're accessing secure, encrypted websites, they know which sites you're visiting, although if the site is secure, they can’t tell what you’re doing. There are several ways hackers can leverage these networks to take advantage of you.

5. Loss or Non availability of evidence

‘Lack of evidence’ is one of the cause of increasing cyber crimes. This also makes difficult to catch the criminal through law. There are different ways to hide and erase the footprints of a cyber crime. To police the cyber criminal at actual is difficult. Take an example of a pedophile –a person who sexually attract the children who traps his victim through social media (email, twitter etc.). The police can find out the information to the criminal, but till permanent physical evidence is not found, the trail or mark cannot be used in a law court.

6. Accessibility to Victims

There are many innovative ways to commit crimes on the Internet than the traditional methods. These crimes are invisible as done through internet or computers. These crimes are also called as ‘White Collar crimes’.

The number of people surfing online allows cyber criminals to point out their victims. There is no need to be present physically. Criminal remain unidentified which push him to commit more crimes online. Police find it immediate difficult to locate people when the trail or mark is online. The examples includes as follows:

- Child or teenager pornography, pedophiles (people who are sexually attracted to children) trap their victim's online.
- Rapists do sexual attacks by finding victims through social networking sites.
- There are Hackers who collect information online by various means and use it at their level for criminal purpose. For this they do not need to be a part of authentic network.

Though technology has made advancements, it will not be easy to catch theses cyber criminals immediately by Police force.

7. Jurisdictional uncertainty

The laws can bind criminals when evidence is there. But in case of cyber crime cases due to lack of evidence, law loses jurisdiction in the court. This is one of the main reasons of increased cyber crimes which occur through online access.

- **UNIQUE FEATURES OF CYBER CRIME**

Computer crimes have some unique characteristics which may be stated as follows:-

1. Computer crimes have now become a global phenomenon which does not have any territorial barriers of jurisdictional restrictions.
2. Another feature of cyber crime is non- existence of any physical evidence of it. Unlike a traditional crime, where the evidence can visibly be seen and felt in form of weapon , blood, stains, finger prints, DNA etc. the cyber crime does not leave any such physical evidence to indicate its occurrence. The evidence in case of cyber crime being in the digital format can be identified only by specially trained and skilled computer users.
3. The perpetrators of cyber crimes are generally highly intelligent educated persons who cherish a challenge. They are well conversant with the operation of the computer system and its intricacies..
4. Some of the cyber crimes are not really new in substance, but the medium through which they are committed is new. Some of the newly arrived cyber crimes are electronic vandalism, cyber terrorism, transnational crimes in cyber space etc.
5. The medium for cyber crime being computers network system, it does not require the user to disclose his identity. Therefore, cyber criminal can conveniently manage his anonymity, which enables him to remain out of reach of the law enforcement agencies.
6. The computer network has created new potential to commit traditional crime in non-traditional ways. E.g. Cyber terrorism, cyber fraud, money laundering, theft of data, cyber pornography, counterfeiting by using computers etc. are some of traditional crimes which are now committed online through electronic media.

Why is a Special Program for Cyber Security needed?

To combat information security threats, only Anti-virus software is not the complete solution. Security threats can travel from any location. It may be inside or outside of the network. Information can be stolen or obtained in illegal ways from anywhere. It may be network, laptop, desktops, company servers, Internet, LAN, WAN or MAN type of networks. Therefore, there is need to identify channels from where information can be stolen. The devices may be USB ports, wireless access to computer systems, networks, Voice over Internet Protocols (VoIP), desktops, laptops, smart phones etc. Information can be hacked from most of these devices.

- **CLASSIFICATION OF CYBER CRIMES**

With the expanding dimensions of cybercrime it became necessary to analyze as to how these crimes vary in nature and form. Therefore, different actions which may amount to crime criminally have been broadly classified into three main categories as follows:

1. Cybercrimes where computer is used as target.
2. Cybercrimes where computer is a device facilitating the crime
3. Cybercrimes where computer is incidental to other crimes.

1. Computer as a target for the crime :

In this type, computer is the target of the crime. The crimes which are covered under this category are:

1. Damage of Computer systems or computer networks.
2. Damage of O.S. (operating systems) and programs.
3. Data Theft or stealing of information.
4. Theft of intellectual property such as programming code or computer software.
5. Theft of information related to marketing.
6. Blackmailing to individual or organization which is based on information gained from computers such as financial information, personal history, sexual preferences etc.

2. Computer as an instrument facilitating crime:

The growth of computer has generated new types of traditional crimes. For example, software piracy, imitating, copyright violation of program codes, computer programs, theft of technological equipment are covered under this category of crime. Sale of copied database is example of computer crime of this type.

3. Computer is accompaniment to other crimes:

In this type, computer is not required for the crime to happen. But automation or computerization helps in the incidence of crime by processing of enormous amount of information and makes the crime more difficult to be traced and identified. The best example of this type of crime is money laundering. An illegal banking transaction happens using the same manner.

- **TARGETED SEGMENTS OF CYBER CRIMES:**

The segments which can be targeted are compared as follows:

Table 3: Target Segments of Cyber crimes

Cyber crime against person or individual	**Cyber crime against property**	**Cyber crime against state or society**
Harassment via e-mails	Computer Vandalia	Intrusion of Computer system to extract secret information.
Cyber stalking	Virus transmission	Cyber terrorism
Dissemination of obscene material	Denial of Service attack (DoS)	Distribution of private software
Defamation	Unauthorized or illegal access over computer system	Contaminating youth minds by through inappropriate exposure
Unauthorized control/access over computer system	Intellectual property crime	Illegal human trafficking on line
Indecent exposure	Internet time theft	Financial scams and frauds
E-mail spoofing	Sale of illegal articles	Sale of illegal articles
Pornography (basically-child pornography)	Sending pornographical Messages, pictures	On-line gambling

Note: The offences shown in the above three categories are only illustrative and not exhaustive.

- **SCOPE OF CYBER LAWS IN INDIA**

IT (Information Technology) Act established in 2000. From that time Cyber Laws and its study got significance in India.

Traditional crimes such as forgery, mischief, defamation, fraud comes under Indian Penal Code. Cyber crimes consist of all above traditional crimes and hence all comes under Indian Penal Code.

Cyber law handles legal issues. The legal issues involve the disputes or crimes aroused from the use of communications technology. These crimes are noted by the Information Technology Act 2000.

Compliancy to cyber laws is essential for everyone. They may be people, individual, corporates or small or large businesses. Therefore awareness of cyber laws also becomes important one.

The main Acts related to Information Technology are

1. HIPPA Act also called as Health Insurance Portability and Accountability ActCompliancy
2. GLB Act also known as Gramm–Leach–Bliley (GLB)Act Compliancy
3. European Union's (EU) Privacy Directives Legislative Act.

Every business must follow these acts related to Information technology. Compliance of these acts in business is must. Otherwise it may prove as risk to businesses.

HIPPA Act:

Confidential Data of person is saved under HIPPA- the Health Insurance Portability and Accountability Act. This data is sensitive as it has details of person and his health record. The HIPPA rules includes saving the medical and personal information. It gives access to this saved data. Access to the data is possible when needed.

The HIPPA guidelines created for security mainly outlines standards of national security to protect Person’s health data which is electronically saved or accessed or transmitted electronically. Therefore it is also known as ePHI i.e. electronic Protected Health Information.

GLB Act Compliancy:

GLB Act (Gramm-Leach-Bliley Act or GLBA) is popularly known as the ‘Financial Modernization Act’ established in 1999. It is a federal law enacted in the US. The objective of this act is to control the methods or ways in which financial institutions deal with the private information of organizations or individuals.

The GLB Act consists of three sections mainly:

1) The Rule of Financial Privacy:

This rule regulates or controls the collection and disclosure of private information related to finance.

2) The Safeguards Rule:

This rule states that financial institutions must implement and adapt security policies to protect such information.

3) Provisions of Pretexting:

This section prohibits the practice of pretexting. It is to accessprivate information using false pretenses. The Act also demands financial institutions to give stakeholders official privacy notices that explain their best practices related to information-sharing and other do’s and don’ts.

`

Trends of ICT in India-2006, 2007 and Trends of Cyber Security as explained by PTLB-2007, etc. have proved that India has to pay complete attention to the legal structure or framework. The legal framework will enable the Information Communication Technologies (ICT) systems in India. India has very weak cyber security system which will worsen the situation.

Perry4Law

Perry4Law is the topmost firm of India. It is in Techno-Legal domain. It provides services related to 'Electronic Services Delivery' and deals with issues related to ICT. These are issues in Banking and Finance sector, Business framework, Advisory of Corporate and Commercial sectors, Contract Management, Cyber Law, Due Diligence, Digital Evidence, E-Courts, E-Commerce, E-Governance, E-Discovery, Corporate, Inbound-Outbound Investments, Portfolio Management Intellectual Properties, Acquisitions and Mergers, NEGP i.e. National E-Governance Plan. , Online Dispute Resolution, Legal Enablement of ICT Systems in India, Equity and Venture Capital in private sector, Technology related disputes, Domain Disputes Resolution and others.

- **LAWS APPLICABLE TO CYBER CRIMES**

1) Section 65 :

This section refers to 'Tampering with Computer Source code'.

Who is liable?:A person who knowingly or intentionally seals, destructs or changes or knowingly causes another to destroy or change any software source code used for a computer or Computer program, computer system or network.
Punishment: Imprisonment up to 3 years
Fine: up to Rs. 2 lakhs or both [imprisonment and fine].

2) Section 66:

This section refers to Computer Related Offences:

Who is liable?: If any person, does any act dishonestly or fraudulently, referred to in section 43, he shall be punishable.
Punishment: Imprisonment for a term which may extend to 3 years
Fine: Fine which may extend to rupees 5 lakh or both [imprisonment and fine].

3) Section 66A

This section refers to ‘Punishment for sending offensive messages through communication service etc..

Who is liable?: Any person who sends offensive messages by means of a computer or any communication device, is liable to punish under Section 66A

Punishment: Imprisonment up to 3 years

Fine: Fine may extend up to rupees 1 lakh.

4) Section 66B

This section refers to ‘Punishment for dishonestly receiving stolen computer resource or communication device.’

Who is liable? : Any person who dishonestly receives or stores any stolen computer resource or communication device knowingly shall be liable to punish.

Punishment: Imprisonment up to 3 years

Fine: Fine may extend upto rupees 1 lakh or both (imprisonment and fine).

5) Section 66C

This section refers to ‘Punishment for Identity Theft’.

Who is liable?:A person who dishonestly or fraudulently makes use of the electronic signature, such as password, card number or any other unique identification feature of any other person, shall be liable to punish.

Punishment: Imprisonment for a term which may extend up to3 years.

Fine: Fine this may extend to rupees 1 lakh

As per the Center of Non-profit Identity Theft Resource (NITRC), identity thefts are divided into four categories. These are identity theft related to finance, identity theft related to crimes, cloning of identity and identity theft related to business.

6) Section 66D

This section refers to 'Punishment for cheating by personation by using computer resource'.

Who is liable?: Any person who by means of communication device cheats by identity theft shall be punished.

Punishment: Imprisonment for a term which may extend to two - three years.

Fine: Fine this may extend up to1 lakh rupees.

7) Section 67

This section refers to 'Punishment for publishing or transmitting obscene material in Electronic form'.

Who is liable?: Any person who publishes or transmits any material in the electronic form, which is lustful or invokes to the sexual interest or if its effect is such as to tend to deviate and deviate persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or incorporate in it, shall be liable to punish.

Punishment: On first Conviction, imprisonment up to 3 years, On Subsequent Conviction imprisonment up to 5 years

Fine: On first Conviction fine up to Rs. 5 lakh, On Subsequent Conviction fine up to Rs. 10 lakh

1.3 ORGANIZATIONS DEALING WITH CYBER CRIME

Cyber crimes occurred during last 5 years (2011-16) have been studied by referring to standard National and International reports. Following standard reports have been studied for getting broad spectrum on cyber crimes.

1) NCRB (National Crimes Records Bureau, Ministry of Home affairs,
Govt. of India, Delhi) reports during 2011-16

2) NASSCOM (The National Association of Software and Services Companies)

3) DSCI (Data Security Council of India)

4) Symantec India

5) FBI (Federal Bureau of Investigation)

6) Cyber crime statistics given by Directorate of Forensic Science Laboratories, Home Department, Santa Cruz (E), and Maharashtra state Dt. 7.11.12.

7) Cyber crime report on Data theft, Phishing, Credit card registered under IT Act received from Cyber Cell, Crime Branch and Thane from Government Information Officer (Dt.22.11.2012) for the period 2009-11.

8) Cyber crime report on E-mail threat, data theft, website hacking, phishing, Credit card Fraud received from Cyber Cell, Crime Branch, Mumbai from Government Information Officer (Dt.26.11.2012) for the period 2009-11.

Reports of these organizations highlight:

1) Different types of cyber crimes

2) Cyber crime trend

3) Rate of cyber crimes

4) Cases reported and investigated

5) Pending cases

6) Reasons of pending cases

All the above reports helped to identify the following:

1) Most frequent cyber crimes

2) Impact of cyber crimes on Organization / Individual

3) Problems occurring in investigation of these crimes

1.4 MOTIVATION FOR RESEARCH

Annual reports published by NCRB, DSCI, Symantec, FBI, and NASSCOM for last 5 years highlights the increased rate of cybercrimes in society at large.

IMPACT OF CYBER CRIMES

Cyber crime affects the individual, group or organization in many ways like data/money loss, theft, defamation etc. The statistics of cyber crimes of last 3 years (2009-2011) highlights the increased rate of crimes in society. It needs to be controlled proactively as it is responsible for affecting nation, individual or organization.

Despite increased awareness of cyber crime, cyber attacks continue to spread in every sector. Mitigation of cyber attacks is a challenging task. Out of many efforts to prevent cyber crimes, most important is 'Effective prosecution of cyber crimes.'

Reports published by government of India give clear picture of cyber crimes in all states of India. Alarming rate of increase in cyber crimes in Maharashtra, Karnataka, Andhra Pradesh, and Uttar Pradesh is of serious concern. This problem needs attention of all entities related to cyber crime like Police, Suspect, Plaintiff, Society, Technical experts, Judiciaries etc.

The rise in cyber crimes in last 10 years raises the following questions:

1) Why there is no control on increase of cyber crimes in India?
2) Why there is inverse proportion of cases registered and persons arrested under cyber crime?
3) Why certain states have highest no. of cyber crimes?
4) Why there is rise in cyber crimes in some cities in last 3 years?
5) Why cyber crimes of particular type are increasing in society?
6) What is the motive behind cyber crimes?
7) What are the social, legal, technical aspects and obstacles in investigation of cyber crimes?

All these questions prompt the researcher to analyze the factors affecting effective investigation of cyber crimes in India, its possible impact on investigation and solutions to it.

With more and more people relying on communication devices like computers, mobile phones, internet etc. the frequency of cyber crimes is certain to increase in future. Therefore it is important to analyze factors affecting investigation of cyber crimes and the impact of proposed solutions.

1.5 NEED OF RESEARCH

It has been observed from NCRB's (National Crimes Records Bureau of India) reports that Cyber crimes committed in the age group of 18-30 years are more than age group of 30-45 years.

The motive behind these Cyber crimes is greed, money, revenge, extortion, cause disrepute, satisfaction of gaining control, fraud, illegal gain, and harassment etc. according to reports of NCRB.

The crimes committed in Maharashtra are highest as compared to other states in India.

In Maharashtra, Pune has the highest no of cyber crimes. Pune city is growing in all aspects may be Educational, Cultural, Industrial etc. due to its conducive environment.

Pune being IT hub is facing a problem of increasing cyber crimes in last 5 years. This fact is supported by NCRB (National Crimes Record Bureau) of India which has highlighted that Cyber crimes in Pune region are increasing at an alarming rate in last few years.

Therefore it is important to find out the reasons of increasing cyber-crimes in Pune.

Some reports from various cyber cells of Maharashtra obtained under RTI (Right to Information) Act. These reports reveals that there is inverse proportion of Cyber crimes registered, Crimes investigated, Crimes under investigation and Pending cyber crimes.

This has motivated to do the research in the area to find out what are the factors responsible that affect effective investigation of cyber crimes.

1.6 SOCIAL RELEVANCE OF RESEARCH

In today's dynamic environment, cyber security has become vital for individuals and families, as well as organizations. Organizations vary such as military, government, business, educational and financial institutions etc.. These organisations collect and store a wide range of confidential data on computers and transmit that to other computers across different networks.

For families, protection of children and family members from cyber crime has become substantially important.

For an individual, protecting information that could impact social life as well as personal finance is essential. One must understand the difference between virtual and real world.

Cyber security is equally important for local, state, and central government as these organizations maintain a huge amount of confidential data and records concerning the country and its citizens. Stealing of confidential data or sensitive information, digital by terrorists from government organizations, as well as digital spying can lead to serious threats on a country.

In this context, this research highlights important aspects of Cyber crimes, cyber security, awareness, its investigation process, status, preventive measures and other related concern areas.

1.7 OBJECTIVES OF THE RESEARCH

The objectives of the research are:

1) To find out ‘Cyber safety Awareness’ amongst people of age group of 18-30 years and above 30 years.
2) To find out the crimes registered and crimes investigated in all Cyber Cells of all Police stations of Pune city.
3) To find out factors affecting effective investigation of cyber crimes in Pune region from experts in this area.
4) To impart training to school children of age below 18 years so that they will be more aware on cyber safety and cyber crimes.
5) To propose a model for cyber crime investigation process that will help all Cyber cells, Cyber Forensic Lab and Police stations of Maharashtra for timely investigation of cyber crimes.

The outcome of this study will help to improve success rate of cyber crime investigation process and decrease rate of cyber crimes in society.

CHAPTER 2 –LITERATURE REVIEW

This Chapter is discussed under the following heads

2.1 What is Literature Review?

2.2 Part-I –

- Survey of International Reports
- Symantec Global Internet Security Threat Report
- Quick Heal Report
- VERIZON's Data Breach Investigations Report
- FBI Report

2.3 Part-II – Survey of Reports in India

- Report of NCRB
- Report of DSCI
- Report of NASSOM
- Report of Cyber Forensic Lab, Santa Cruz (Maharashtra)
- Report of Cyber Crime Cell, Thane (Maharashtra)
- Report of Cyber Crime Cell, Mumbai (Maharashtra)
- Report of Cyber Crime Cell, Pune(Maharashtra)

2.4 Part- III

- Research papers/Articles related to Cyber crimes:
- Cyber crime and security Cyber Attacks
- Cyber crimes in India
- Legal dimensions of cyber crime

2.5 Gaps identified from the review of Literature

2.1 What is Literature Review?:

A review on Literature is a survey and observation of literature in a particular area of study. A literature review consists of study of various surveys, journals, books, articles, research work related to area of study. It develops the deeper understanding of the subject and expands the knowledge horizons of the area under study.

The literature review for the present study has been carried out in three parts- Part-I, Part-II and Part-III.

2.2 Part-I - Review of International Organizations working for Cyber Security

There aremany International organisations which are specifically working on information and cyber security. The work of these organisations reviewed through many reports to get understanding of severity of problem on global platform. Authentic work done on Information security is reviewed using many conferences/research papers and journals. Amongst these organisations, reports of Symantec, Quick Heal Technologies Ltd., Verizon Corporate and Federal Bureau of Investigations are studied from research point of view.

SYMANTEC CORPORATION (USA)

About Symantec

Symantec Corporation based in United States is the world's top most leading cyber security company. It allows organizations, governments and people to secure their most important data. The data is wherever organisations or people exist. Enterprises all over the world across the world rely on Symantec for integrated cyber defence against sophisticated attacks such as cloud, across endpoints and infrastructure.

Symantec India:

Symantec India is present in Pune and Chennai. It is one of the largest Symantec Research and Development centres with a team of more than 2000 engineers focused on products and services for international markets.

Symantec Report:

Report of Symantec (2015) on “Global Internet Security Threat Report” gives an overview & analysis of global scenario of Information security threat activities on annual basis.

This report provides required information to small businesses, enterprises and consumers about how to protect and secure their systems at present and in future.

Symantec records numerous events per second through the “Global Intelligence Network”. Threat activities in over 150 countries and various territories is monitored by this network. This information provide Symantec analysts additional sources of data to analyze, identify and provide emerging trends in Cyber Security such as phishing, cyber attacks, malicious code activity and spam.

The annual Symantec Internet Security Threat Report (2015) highlights multifold information including targeted attacks, threats to smart phones, scams through social media and Internet of Things (IoT), vulnerabilities as well as attacker’s tricks, motivations for cyber attacks and behaviours of cyber attackers.

Key findings of Symantec’s Internet Security Threat Report (2015) on cyber security are as follows:

1) Billions of Personal / organisational records were stolen or lost in the year 2015.
2) As website administrators fail to secure their websites, Cyber criminals are encouraged to take due advantage of Vulnerabilities in authentic or government websites. The purpose is to

infect users. Cyber attackers are targeting government organizations or financial organisations. They target not only Fortune 500 companies but companies of all sizes

3) Cyber criminals are using Encryption (technique of encoding data) as a weapon to hold confidential and important data of companies and individuals.
4) As nowadays people are surfing online and spend most of the time on internet, attackers are searching new ways to spoil or destroy property, confidential information or life of victims.
5) Cybercriminals in 2015, 2016 have proved that people's lives are vulnerable online. Data breaches, government supervision, and traditional scams came together to further destroy personal privacy, whether it is personal photos, login details or medical histories.
6) In general people lack awareness on cyber safety. Therefore many scams still continue considering the weak security habits of the people. The criminals succeed in their mission of cyber attack. However websites having weak security are vulnerable to data. This data can be exposed despite of having strong password.
7) Scams on Social networking sites require some form of dialogues or interactions. People share their information to unknown persons through social media. This remained the main cause for attacks of social media.

QUICK HEAL TECHNOLOGIES

Quick Heal Technologies Limited is the leader in Security Solutions. This Company is known for Antivirus and its work in security domain. It is located in Pune, India. It has its presence internationally in more than 80 countries.

The Annual Threat Report 2016 of Quick Heal highlights a detailed insight into the state of digital security. In the year 2016, Quick Heal detected a targeted attack on an Indian government organization. There was one group behind this attack. This group is active since 2010. This group is famous for a reputation of having attacked government agencies and embassies of various countries in the past. This group targeted an Indian government organization in 2016 using phishing technique i.e. through e-mails.

In 2016, Quick Heal lab had also came across a targeted attack. This attack was aimed to target at a private online marketing firm that caters to small businesses in the U.S. To make the attack that will look more legitimate, the cyber attackers first gathered from social networking sites various details about the company and the company's website.

These documents were then sent as an attachment in spear emails to the employees of the company. When these documents were opened, the attackers were able to compromise and get the organisation's system and hack confidential business information.

This report is a good example of how attackers are finding the vulnerabilities to attack organisations. Organisations showed lack of security system to identify fake, illegitimate mails through company's mail server.

Quick Heal has a research department which carries out threat research, threat intelligence and cyber security. To deliver timely and improved protection to its users, Quick Heal Security Laboratories do analysis of data which is retrieved from Quick Heal's products all over the world.

Quick Heal Quarterly Threat Report- Q2 (2017) has highlighted following observations.

1) Although malware detection in Windows and Android operating systems in Quarter-2 lowered down compared with the previous quarter, ransom ware attacks have increased. There have been 5 attacks so far with WannaCry and Petya.
From this trend it can be said that attackers are shifting their attention towards attacks that give them more money in most easy form. Ransomware attacks have higher returns compared with data stealing and other malicious campaigns.
With Ransomware as-a-Service means a service where malware owners sell ransomware for free or for a small charge or fee gaining the foundation to novice cyber criminals who are infecting computers and extracting money from their victims. In short, the ransomware business is a fast growing in present scenario.

2) More than 160% increase in Banking Trojans in Quarter 2016 using Android platform could be boon for attackers taking advantage of the ever increasing popularity of digital payments. As more users run towards mobile banking apps, they go nearer to the periphery of cybercriminals.

Report at the end concludes on following notes:

1) With the number of ransomware attacks witnessed so far, 2017 may well be dubbed as “The Year of the Ransomware”. Cybercriminals are trying to make their lives easier by working on attacks that require fewer resources but at the same time, give higher returns. And this is why ransomware is becoming a dreaded nightmare to individuals and businesses across the world.

2) With increased digitization, people are sharing their personal data more than ever. And data is seen as a gold mine by attackers and ransomware is their tool of choice to extract this gold.

3) WannaCry couldn’t have been the biggest attack in history if people were prudent enough to keep their Operating Systems up-to-date with the security patches which Microsoft had released way before the attack happened. This was a disaster which could have been easily avoided – again a screaming reminder that humans still are the weakest link in computer security.

4) It’s about time we paid heed to warnings, understand the types of digital threats that surround us, be wary of sharing our personal details and treat our digital lives in the same manner as we treat our real lives – with a sense of security.

VERIZON CORPORATE

Verizon Corporate is one of the biggest communication technology Industries. It is located in U.S.A..Company has taken leadership in Communications sector which is innovative and emerging field. It is also leader in Technology solutions and services. It is a Global leader in Innovative communications and technology solutions and Services. Every year it finds data breaches.

Investigations Report of 2015 on Data Breach recently published by Verizon. This report shows that cyber criminals rely on promising techniques of Phishing to break organisation's security. The nature of attacks is becoming complex. Still the cyber criminals rely on phishing techniques.

This report highlights that many organizations, industries taking efforts on defence related to social engineering. Most of the (25%) recipients are opening phishing attachments and out of 25%, 10 percent recipients are clicking on attachments which they should not. Therefore Verizon report says that Phishing is increasing continuously. Therefore defences related to social networking crimes should be improved at faster speed.

Bareja (2015) is treating 'awareness' as critical component in the Verizon's report on Data breach published in the year 2015. In a strategic planning to combat rising cyber threats, awareness is most important factor. He further adds that embedded softwares should be developed here onwards considering security challenges. Client-Server softwares should be developed in the same manner. In India we treat this as acceptance of risk to avoid either our inconvenience or ignorance.

Gogia (2015) says further in this report that Companies, organisations are investing highly on technology. But technology alone is not only solution to avoid cyber threats. He said that organisation should also invest on people and training.

FEDERAL BUREAU OF INVESTIGATION (FBI)

The **FBI** is the USA's law enforcement agency. It is a first domestic intelligence and security service of the USA.

The FBI basically serves their citizens who victimize the cyber crimes through inappropriate use of the computers on technology. This organisation serves their people buy creating awareness on cyber challenges and their consequences.

The FBI takes the initiative for investigation of cyber attacks by cyber criminals and cyber terrorists. Cyber threats are continuously rising and growing. Invasions into systems are more dangerous and more easy for cyber criminals.

The efforts taken by FBI on cyber security as follows:

- ✓ There are Cyber criminals who want to steal personal information. They want to sell it through black markets. FBI try to totally prevent this by avoiding 'network and computer intrusion' by attackers.
- ✓ There is a division of a FBI related to cyber issues to address cyber crimes.
- ✓ FBI takes Prevention efforts by two ways – by training people/employees on cyber safety awareness and using preventive controls through technology,
- ✓ FBI has 'cyber squads' which are specially trained. Their main role is to protect against computer interventions, data theft, copy of intellectual properties such as trademarks, copy rights; personal information, child pornography and online business frauds.
- ✓ FBI gets cooperation from other federal agencies. They are DoD i.e. Department of Defense, Homeland Security Department mainly. They come together to combat rising cyber crimes.

CNAP:

CNAP means FBI's Cyber security National Action Plan(CNAP). This plan guides the Federal Government to take appropriate action. They keep long term vision for improvements on cyber security. This helps to improve cyber security awareness. This also helps to improve protections of privacy and public safety. This gives economic and national security. This motivates Americans to secure their digital assets. CNAP actions consist of following:

- Form the Commission which will enhance National Cyber security.
- Innovate IT Government by modernising.
- Multiple authentication
- Enhance the Level of Cyber security all over the Country
- Secure Technology in use

CNAP is also training Americans to protect their online accounts not only through passwords but adding one more layer of security to that. A strong password is combined with biometrix such as finger print or code in a text format. By using these techniques, Americans make their accounts more secure. The concept of multi-factor authentication need to be a theme for a Cyber security Awareness Campaign at National level. This plan is guideline for other countries which gives roadmap on updated perspective on cyber security.

The FBI totally denies or does not support ransom to pay to a ransomware attack. This payment does not ensure that organization will get its data back. Few organizations have experienced that they did not get its decryption key back by theses attackers after payment.

Paying a ransom encourages cyber criminals to attack more organizations for money. There is a chain of cyber criminals involved in it. They get incentive for this illegal activity. Payment to such ransom means funding cyber criminals illegal activity.

There are some tips given by FBI to deal with attacks of ransomware. These tips are not only for organizations but for individuals also. All employees of the organization should be aware about the ransomware.

- Patch Management system should be followed in operating system and softwares on digital devices.

- Check and ensure that antivirus updates automatically and scans data regularly.

- Users should be authorised. Authorised users only should Manage the privileged accounts.

- Share permission for access controls to files, directory and network.

- Do not enable macro scripts which are sent through mails from office files.

- Implement effective security policies with other controls to prevent programs or coding from ransomware.

- There should be regular data Backup. Always Ensure integrity of the data for which backup is taken..

- Secure backups. Backups should not be connected to the computers and networks computers.

2.3 PART-II – SURVEY OF REPORTS IN INDIA

NATIONAL CRIMES RECORD BUREAU OF INDIA (NCRB)

NCRB is department coming under of 'Ministry of Home Affairs' of Government of India. Department of NCRB started in 1986. This department has a mandate to train Indian Police with information technology. Technology solutions and knowledge of its implementation enable them to enforce the law more effectively. Along with other types of crimes, It gives statistics of various cyber crimes registered, resolved and pending. The cyber crimes are recorded under IT act under different sections. The data is considered more reliable and gives the present crime scenario in the country.

- NCRB presents annual publication of Crimes in India giving various aspects on crime. This study has given principal reference for cyber crime statistics in India.
- This statistics is helpful in analyzing different trends adapted by cyber criminals in recent years. Also it highlights states of India where cyber crimes are increasing with an alarming rate where great control, special training and education is required to people in society and those who involved in investigation of these crimes.
- This study also suggests having strategy to combat cyber crimes at various levels such as Individual, Group and Organization.

Cyber crime reports of last 5 years (2011-2016) were studied from different contexts
such as:

- Age wise cyber crimes
- Cyber crimes under different sections of IT Act
- Different types of cyber crime
- Cyber crimes with different motives
- State wise cyber crimes
- City wise cyber crimes

DATA SECURITY COUNCIL (DSCI)

DSCI of India is a pioneer industry which protects data in India. This council is set up by NASSCOM (|National Association of Software and Services companies)in the year 2008. Aim of DCSI is to make cyberspace safe and secure. Its aim is to ensure best security practices, maintain standards of safety. It takes initiative in the areas of cyber security. It is working proactively in Data security field. Annual reports of Data Security are published.

According to objectives of DSCI, it campaigns for information security to governments, regulatory bodies and Industry associations on policy matters. DSCI has always maintained its leadership in cyber security and privacy. It publishes periodic reports on security and its best practices.

It also focus on various survey results. It creates frameworks for security policies. It publishes papers and survey reviews for others. DSCI is engaged in Capacity building in security, privacy as well as cyber forensics. It conducts training programs round the year. Some Standard Certification program are created for professionals and law enforcement agencies. It maintains relationship with stakeholders through various initiatives such as mentoring, consultation, events , chapters and memberships to organisations.

Report of DSCI published in 2017 on Growing Cyber Security provides a guideline for the industry. It also provides recommendations to the Government. This helps Government to set up the required ecosystem.

This report is in two parts:

- First part highlights analysis of global market trend related to supply and demand, country & cluster analysis and identifies areas of opportunity for the IT Industry.

- Second Part highlights Perspectives for Government related to capacity building, Policy and its implementation, technology building etc..

NATIONAL ASSOCIATION OF SOFTWARE AND SERVICES COMPANIES (NASSCOM) :

NASSCOM is a non-profit industry association in India. Its branches are in Mumbai, Pune, Bangalore, Chennai, Hyderabad, Kochi, Kolkata, and Thiruvananthapuram.

NASSCOM has its significant contribution in India's GDP. It has influence on exports, infrastructure and employment. NASSCOM since its establishment in 1988 constantly support the IT industry in India.

NASSCOM is taking efforts to make India as a hub for Cyber security. For this it has set up the Security Task Force. Purpose of this is to study the key issues that will make India as a hub for cyber security solutions. This dream will come true with consistent efforts till 2025.NASSCOM by focusing policy regulations making it the integral part of IT BPM industries.

1. NASSCOM is an organisation not meant for profit making. It is sponsored by the industry. Its objective is to develop a growth oriented and sustainable technology in the country.

2. NASSCOM set up a Cyber Security Task Force (CSTF). It is working towards PM’s vision. Vision of PM is to make our country the global hub of Cyber Security. The CSTF is working towards Skills Development, building the capacity of organisation to tackle cyber safety and develop the technology solutions. The objective of the Task Force is to build the industry of cyber security in India.

3. The main aim of CSTF is to create a trained manpower or expert cyber security professionals in millions with certifications and skills. Based on this skilled manpower it aims to prepare more than 1,000 security based product companies in India. NASSCOM takes efforts to publish Annual reports based on latest trends in the area of information / Cyber security.

Report of Cyber Forensic Lab (2009-2011), Santa Cruz (Mumbai)-Maharashtra

This report is received from Directorate of Forensic science Laboratories, Home Department, Santa Cruz, Mumbai, Maharashtra under RTI. This report shows trend of rising cyber crimes from 2009 to 2011. The crimes are mostly related to E-mail theft, Data theft, website Hacking, Phishing, Credit card Frauds. There are huge no. of cyber crimes under investigation. The reasons given by officials are **Inadequate staff** and **Huge receipts of cases** from all over Maharashtra**.**

Report of Cyber Crime Cell (2009-2011), Crime Branch, Thane- Maharashtra

This report is given by Government Information officer and Asst. Police commissioner, Crime Branch, Thane under RTI. This report highlights cyber crimes related to Data Theft, Phishing, Credit Card Frauds. From 2009-2011, out of 24 cases 16 i.e. approx. 66% cases are under investigation which is a serious threat..

Report of Cyber Crime Cell (2009-2011), Mumbai-Maharashtra

Report of cyber crimes received from Cyber Cell, Crime Branch, Mumbai (2012) , given by Government Information Officer and Asst. Police Commissioner, Crime Branch, Mumbai under RTI.

This report shows that out of 14 cyber crimes (2009-2011) related to E-mail theft, Data theft, Phishing and Credit Card Frauds, only 4 cases are under investigation which is only 30%.

Report of Cyber Crime Cell (2009-2011), Pune-Maharashtra

Report of Cyber Crimes (2009-2011) received from Office of Pune Commissioner and Public Information Officer, Cyber cell, Crime Branch, Pune (2012).

This report shows cyber crimes related to Email Threat, Data Theft, Website Hacking, Phishing and Credit card Frauds. Out of these cyber crimes, crimes related to Phishing are highest. Out of 112 Phishing cases in last 3 years, 44 cases are under investigation i.e., 40 % cases are under investigation which is giving space to cyber criminals.

2.4 Part- III Research papers/Articles related to Cyber crimes:

- Cyber crime and Security
- Cyber Attacks
- Cyber crimes in India
- Legal dimensions of cyber crime

Cyber crime and Security

Cyber security is aimed to protect network, data on computers from unauthorized access, It also refers to the technologies and processes to protect vulnerabilities (weakness that allows attacker to reduce security of system) and attacks passed through the internet via cyber criminals.

ISO (27001) is the Standard for International Cyber Security. It is managing Security System. It provides prototype for improving, operating information establishing, implementing, monitoring, maintaining, reviewing an Information Security System.

Sharma (2012) studied various cyber security emerging trends. These trends he considered as mobile computing, cloud computing, social networking and e-commerce. According to

him our “National Cyber Security standard” is identified on how well managed is our infrastructure for handling “Cyber Crimes”.
This paper also highlights the gap between Critical IT Infrastructure and Security agencies and challenges that arise due to lack of coordination between two.

Kareem (2015) in his paper on cyber crime investigation, he studies impact of ICT issues on private sectors and e-Governments. He highlights fast increase of information in the world and communication aids. These aids include hand held technology, network and computers which caused increasing risk of cyber attack. Therefore, issue of cyber security becomes a big. Therefore, he further adds that there is a need to catch cyber attackers. This will help to protect information and minimize the risk of cyber-attack.

Lutta and Obirili (2015) have discussed the Rising Cyber crime Threat for Internet – related Businesses. According to this study, in Kenya online commerce is increased in which is a threat to cyber safety of an individual or an organisation.

According to him macro and micro economy may affect in future. This study found out the type of cyber crime and its impact on online businesses in the Western Kenya. Survey was done by collecting data using interviews, questionnaires and results. It indicated that online businesses were adversely affected by cyber crimes.

What he told was actually happened. Google and Twitter companies given alarming notices that state sponsored cyber attacks may attack further their products and services. The survey on Cyber Safety and Security In India, suggests that the cyber attacks all over the world had increased rapidly.

He added further that it is an alarming call for the cyber security vendors to go for an addition of security layer to their security products and services. Otherwise he said to beready for cyber attacks. He further said that antivirus will not be useful if that cannot detect and eliminate a malware.

Going ahead he suggested that framing of techno legal policy for cyber security will help to combat cyber crimes. Lapse of any point in policy may be risk to the individual or organization from finance or brand point of view. There is need to spread awareness on cyber safety amongst individuals, companies and governments. Every organization must form and follow this policy for cyber security.

Unlike other countries, India needs Chief Information Security Officer (CISO) at organizational level. Culture of CISO is still not found in Government Offices. Dr. Rai has been appointed as the first CISO of India. His appointment was made by the Prime Minister Office (PMO) of India. Though this is a very good beginning, there is need to make quick reforms for this. To appoint Chief Information Officers (CIOs) is must for all Banks. Banks have to follow this implementation. Cyber security of banks in India is therefore in weaker state.

Perry4Law Techno-Legal Base (PTLB)

PTLB is a Techno Legal Institution in India. Perry4Law Techno-Legal Base (PTLB) (2015) in their report on Smart Cities and Cyber Security have expressed their views. The objective of smart cities is to provide a best environment for standard living, for propagating business, health and overall development. Use of ICT is inevitable for Smart cities.

Use of ICTs such as cloud computing, Internet of Things (IOTs), Virtualization carries risks for cyber safety. Report further says that cyber attacks against organization, infrastructure can be predicted or visualized against the use of ICT or technology. This cyber attack may collapse smart cities. Therefore India needs national cyber security policy. Considering the urgent need, formation of this policy is must in India.

Cyber security framework of India needs to be strengthened under the guidance of experts in this field There are disputes between the countries when International legal issues of cyber attacks arise. In this case, it becomes essential that these issues must be solved mutually by both the governments. There is need to create Mutual Law Treaties (MLTs) related to cyber issues. At present this does not exist which is a boon for cyber criminals or attackers.

This has underlined the fact that cyber security related projects in India must be executed in reality. They must also be implemented successfully as soon as possible. Indian Government has undertaken many cyber projects but have not been implemented successfully.

The experts worry about cyber security of smart cities. They feel that this Government is capable and hence must take this issue seriously. This can be done through PTLB. It is a center point of research in cyber security and development. They feel that our country must be cyber prepared to protect people, organizations, small and large businesses. As use of technology such as mobile, internet, computers and other communication devices go on increasing in geometric progression, The cyber crime will also increase if no proper policy on cyber security is prepared and implemented. In this context, drafting "Cyber security Policy" is must. The initiative in this direction has already started but found with some defect in previous policy. So new advanced version which is defect free should be prepared as early as possible.

The expert also suggests dedicated cyber law for India. This is what is required for India now. All comprehensive cyber security policy must be prepared considering contemporary cyber security threats using techno legal framework.

Survey says that as we invest on technology and infrastructure, we must invest on people and training. Cyber Safety awareness must be created. People lack in cyber security knowledge. Organizations should come forward so that they can effectively contribute to the initiatives on cyber security and ultimately the mission of Indian Government to free country from cyber crimes.

Perry4Law (2009) in their report has already suggested '10 Point Legal Framework' for Law Enforcement agencies and Intelligence Agencies in India. However, the Indian Government is working to act upon it and design Techno Legal Framework.

Dalal (2014) in his article states that various projects of India such as Aadhar, National Intelligence Grid (NATGRID) are not governed by any legal procedure or law. They should be actually under Parliamentary Umbrella. These projects should be scrutinized. These projects should be governed by Legal framework. He suggests in short that such intelligence infrastructure of Aadhar or any other project needs transparency to be effective and Accountable.

Dalal (2014) in his article says that "Cyber Security Of Banks" in India Needs to be strengthened. He says that we have paid less attention on Cyber Security of our country. This was not taken care for many years previously by government. They have made our ICT infrastructure vulnerable to cyber attackers. Most such sensitive sector is Banks. Security Infrastructure of Banks is very poor and hence paid for that.

He further adds that no security law for cyber world, creating many troubles for organizations of various sectors and people or individual in India. There is need to form stern as well as effective cyber security law in India.

RBI has issued some cyber safety guidelines to banks. This includes guidelines for online safety, risks related to Technology, frauds in cyber space etc. They have made the appointment of Chief Information Officer (CIO) in banks mandatory to deal with related issues.

However, Banks are less interested or ignore to follow this and as no strict monitoring on this, have made banks to take liberty. Therefore we can say that, there is no law making banks accountable. This is the reason banking frauds are increasing. And hence it has become risk to transact online. Therefore, the online banking system in India is not at all or partially cyber secure.

India is promoting adoption of mobile banking at a larger scale through mobile, internet and other methods of financial transactions. However problems related to cyber security of these are not considered. He further says that online banking transactions are vulnerable. So attackers can make use of that for cyber attacks. Therefore security issues must be ensured as early as possible.

He says that India has not considered the issues of cyber security of internet banking, mobile banking, their legal aspects etc..Digital payment promotion or cashless transactions have made banking cyber security in India compulsory. Banking transactions are not completely secure rather vulnerable which gives chance to cyber attackers. Stakeholders must ensure cyber security of online transferors. Embedded Security aspect in turn will increase trust on online banking.

Cyber Attacks

Cyber attack is also known as a computer network attack (CNA). Cyber attack is destruction of networks, computer systems and technology devices. Cyber attacks use illegal or malicious code to change programming or coding, logic of the program, program data. This results in destructive consequences such as loss of confidential data and result into cyber crimes. Cyber crimes may be data theft or identity theft.

Cyber Attacks on Insurance sector In India

The need of cyber insurance is required. This need in India is realized very recently. In the developed countries, they have already adopted cyber insurance.

Indian insurance company’s business has grown enormously and has been well managed by Indian Government. Insurance business in India is well framed and it is also well established in India. With the flow of time, new challenges and opportunities are open for the insurance business. One such opportunity is coming from acceptance of information and communication technology (ICT).

Perry4Law (2004) has been point out use of cyber insurance since 2004. From the inception of cyber insurance and onwards, Perry4Law is observing the developments at national and international levels

Dalal (2014) in his article on Insurance policy, expressed his views on IT Act-2000. It emphasis on adoption of sufficient cyber security practices by companies in India. Cyber security related compliance need to be observed for technology and financial institutions. It should be well observed for e-commerce websites.

A special attention must be given to the rules and practices for cyber safety and personal sensitive data by people involved in technology related business in India.

According to **Indian Companies' Act**, it is the liability of directors to follow cyber law.

They need to follow legal obligations while performing company's daily functioning.

According to this Act, it is mandatory for Foreign Companies to register in India. This is also applicable to e-commerce websites who are doing businesses in Indian market. This mandate will make them accountable for legal obligations and subsequently its compliances. There are few instances where targeted company because of cyber breach has been exposed for litigation in most jurisdictions all over the world.

Cyber security breaches in India would give birth to complicated cyber law issues in the near future. E-commerce business carries many cyber security related issues. These issues must be noted by Government of India as well as insurance companies. Similarly, while doing online payment, all required guidelines must be followed by payment makers. Maintenance of digital documents should be under corporate laws and inspection of documents should be under corporate laws of India. Digital documents have issues like confidentiality, information protection and cyber security.

All these important points should come under techno legal framework. India needs working on this proactively. There are many corporate frauds. India needs updated scientific technologies for investigations. Cyber forensic technologies for search and seizure operations must also be updated as per advanced countries.

The volume and outspread of cyber security issues are considered, Indian Government, corporate sectors and insurance companies need more vigilance. Revenue generated by insurance companies is very good. Hence if cyber insurance has to be potential source of revenue by insurance companies, then it need to be protected by Indian companies. There is need to work hard in this direction.

There are many technical and legal issues involved in international cybercrimes. Entering into insurance agreement is not only sufficient. It will create problems than solutions. The two entities – one insurance company/companies and other affected company/companies may have to face conflict of laws because of lack of mutual law treaties. Other problems include authorship of cyber-crime and attacks, non-cooperation by foreign governments and companies during cybercrimes investigations.

In such situations it becomes necessary to draft proper insurance agreements between two parties. In such situations, the agreements of cyber insurance must be properly drafted by insurance companies. They need to use techno legal skills required for investigation of cyber crimes. This legal document can be or must be used by both the parties- one affected companies and other insurance companies in case of cyber attack cases.

Perry4Law Organization (2015), published the research article on “Prospective Cyber Security Trends In India”. This article states that cyber attacks sponsored by would increase in future. This has happened in reality. Some Social networking sites e.g. Twitter and search engines e.g. Google have issued warnings to people that their products and services may have a fear of cyber attacks.

Perry4Law in 2016, published research article on “Cyber Security Trends In India”. In it they have brought to the notice some issues. It includes rise of malware (Software to damage Computer system/s). Along with this they highlighted botnet (malicious software which infected network system of computers) and cyber-attacks against complicated infrastructures around the world.

It is an alarming situation and wake up call for the Vendors. Either they can make improvement in their security products and services or become ready to go from the market. Only antivirus is not sufficient to combat cyber security threats.

There is need to imbibe security culture in Individuals, organizations, companies and governments. They should frame the techno legal policy for cyber safety. This policy should be strictly implemented. While framing the policy the care must be taken that there should not be any lacuna while framing the policy. Otherwise is will affect the brand value or financial part of the organization.

Perry4LawOrganization (2016) in their report expressed that India needs to inculcate the special Information Officer. In India, many departments still have not recruited CISO.

Recently in India, Dr. Rai has been appointed as CISO. . This is a very good move. For every bank appointment of CISO is must. This is made compulsory for them in 2012. Many banks have not done the compliance of this. Report says that cyber security in banks is weak and needs to be strengthened.

There is need to disclose cyber breach norms in India. Even the few government projects failed to do that. Therefore the chances of cyber attacks would go on increasing. We have been missing proper infrastructure or framework of cyber security in India that needs to be reframed immediately. As we are moving towards, **Digital India**, this practice will help to remove vulnerabilities and in turn threats will be avoided.

Cyber Attack of WannaCry ransomware

Recent buzz word of cyber attack is the WannaCry. It is the ransomware program used globally. It was launched in May, 2017. It infected many lakhs of Systems demanding a ransom to open the victim's files. Hackers demanded money in the crypto currency in many languages. Along with other methods, the method used for the cyber attack was Phishing emails on the systems. These systems are without updated security patches. Experts predicted that this may be continued further to infect more new systems in future. NCA i.e. National Crime Agency is working to find out responsible group behind WannaCry ransomware.

- Cyber attacks have following consequences:
- Website hacking Identity theft
- Phishing Fraud
- Extortion
- Spamming, spoofing Trojans and viruses
- Hardware (laptops, Mobile) Denial of Service Attacks Sniffing
- Data Breach
- Unauthorized access

Dhamija and Tygar (2005) in their research paper on phishing "The Battle against Phishing: Dynamic Security Skins" have suggested new innovative way to save from cyber attack. They suggested new technique. It is called '**Dynamic Security Skin'.** This technique allows a server at remote location to prove its identity. It is very easy to identify for human and hard to identify to cyber attacker for spoofing or phishing. Authors suggested two new techniques for spoofing prevention. In first, the browser provides a window for User name and Password entry. In second, they used a photographic image between the user and Window instead of user id and password to avoid cyber attack.

Parno and Perrig (2005) in their paper "Phool proof Phishing Prevention" have developed a unique system that avoids reliance on user behavior. It protects a user's account even in the presence of key loggers. It protects account from other spyware form as. Authors prepared the practicality of the system with a working model or prototype. The system avoids the reliability on the user during authorization process. This enhances security. This technique eliminates many phishing frauds.

Cyber Crimes in India

Dasgupta (2009) in his book "Cyber Crime in India: A Comparative Study has defined the meaning of cyber crimes, its scope, characteristics and elements. He commented on the scope of cyber crimes. He said that world war will not use weapons here onwards. The world will be driven here onwards with ones and zeros. The war will not be based on bullets. It is now who protects information, controls information. Authors focused on modus operandi of frequently occurred cyber crimes such as cyber hacking, cyber terrorism cyber fraud etc.. They highlighted the efforts taken for prevention of cyber crimes at national and international levels.

Kumar, Koley and Kumar (2015) in their paper titled **"**Present scenario of cybercrime in INDIA and its preventions" have discussed many cases on cyber crimes. All these cyber crimes aroused due to lack of proper knowledge or awareness of cyber safety. They focused on preventive measures for acts which are unlawful. They suggested updations of cyber laws along with change in time.

Vyas and Vyas (2015) in their paper titled "Virtual Parliament – An immediate need of Digitally Ready India" give a visualisation of Virtual Parliament concept. For this, he emphasized to be digital. We need to be digital for the success of Virtual Parliament System if implemented. This is possible and successful when we learn to be cyber safe.

Legal Dimensions of Cyber Crime

Dalal (2015) in his article on "International legal issues of Cyber attacks" presented that Internet is must and unavoidable all over the world. Cyber space is a collective area where the virtual boundaries of various Countries are connected to each other. This connectivity has given many opportunities and benefits to citizens on Net also called Netizens. This connectivity has also given birth to for crimes on Internet called cyber crimes.

He added that new cyber crimes namely Cyber Espionage, Cyber warfare, Cyber Terrorism are dangerous and have very serious effect. For this he suggests to have knowledge to tackle these cyber attacks. There is also no common law or treaty that is acceptable all over the world. Also importantly, there is no ownership, authorship for cyber crime. There are many reasons which made cyber security issues and International laws more complicated. Protection of Confidential data is important for every government all over the world.

He states that in such scenario, managing legal issues of International level of Cyber Attacks are difficult to manage because of different safety and security policies of related countries. India needs to be cyber prepared to face such problems. Despite all obligations, it is not easy to catch cyber attacker.

Author further explains about "Net Neutrality" that when is in danger, emphasizing or insisting our own Standards and Measures against Cyber Attacks by any Country in the world should not be encouraged. It is a need of an hour that countries should come forward. It a high time to resolve International Legal Issues of Cyber Attacks at a global scale

Ryder (2001) in his book on "Cyber Laws (IT Act, 2000), Data Protection, E-commerce and the Internet" has pointed out some issues of concern related to IT Act. He had also suggested the corrective reforms to strengthen the cyber law.

Loader and Douglas (2000), in their book "Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age" has emphasized on cyber crime legislations. He suggested this using philosophy "proper implementation of law in its letter and spirit is more important than its enactment". Further, he highlighted that law enforcement agencies have to play important role in investigating cyber crimes.

Yadav and Arora (2014) in their paper titled "Cyber Crime and Security" authors highlighted to understand the national and international consequences of growing cyber threats. They further added that there is a need to assess the requirements of cyber crime investigation devices all over the world during cyber attacks. This will help to form a uniform legal foundation.

This paper provides a comprehensive outline of the most important and relevant issues associated with the legal aspects of Cybercrimes. It concentrates on the requirements of developing countries for resolving cyber attacks. Because of the global spread of cyber crimes all over the world, the legal actions are more or less same for developing and developed countries

Paranjape (2010) in his paper titled “Legal dimensions of cyber crimes and preventive laws” with reference to India reveals important aspects of cyber crimes. He explains the scope, characteristics and reasons of cyber crimes. He highlights modus operandi of cyber crimes. In a separate chapter on ‘Judicial response to cyber crimes’, he explains challenges before the Judiciary. He highlighted judicial trend in India.

Author highlights ‘Global perspective of cyber crimes and related laws’. The objective of global perspective is to combat rising cyber crimes through International Cooperation. In this context he had comprehensively discussed on various happenings on cyber crimes through national and international conferences, summits etc.. He also highlighted the cyber legislations of different countries like India, UK, Germany, Australia, Canada, USA, China, Japan and France etc. His expert views on all above helps to understand the reason behind rising crimes and where the speed of cyber crime investigation is affected.

Sood (2010) has written a book titled “Cyber crimes, electronic evidence and Legal issues in Investigation”. This book highlights Nature and Types of Cyber crimes in a detailed way. Further he focused on Critical analysis of the cyber crime investigation. He covered an important aspect on leading electronic evidence in the court. There is need to train Police officers to collect electronic evidence from the computers.

He has suggested various methods to combat cyber crimes. Since cyber crimes are based on technology, so the best solution to the problem is implementing security technology to avoid cyber crimes. These security technologies include Fire-walls, anti-virus softwares. He suggested that “**protect yourself”** is the best strategy against cyber crimes. According to author, effective relationship between the law enforcement agencies within the country and between nations for cooperation on legal issues is very necessary to challenge cyber criminals. This will help to bring them before the law.

Mali (2012) in his book “Cyber Law &Cyber crimes” elaborated all types of cyber crimes with definitions, law as applicable and illustrations. This book gives very good insight on ‘Search and Seizure of Digital Evidence’. His valuable tips to prevent cyber crimes are very useful. In a special chapter on ‘Challenges of fighting Cyber crime’ he touches on almost all aspects. Author’s in depth knowledge helps to study research topic on ‘factors affecting effective investigation of cyber crimes’ with valuable inputs.

Kamath (2009) in his book on Law relating to Computers, Internet and E-commerce “A Guide to Cyber Laws and the IT Act, 2000” has expressed his views on the upcoming field of ‘E-evidence’ in the cases of cyber crimes. He has made an in-depth study about the acceptability and reliability, authenticity of electronic records, immense problems of proofs in cyber offences, and effect of such evidences, video-conferencing, forensic computing and best evidence policy or rule etc.

Verma and Mittal (2004) in their book “Legal Dimensions of Cyber Space” have explained the fundamental concepts of cyber world like its meaning, types of cyber crimes, its features and main parts or components of computers; history and growth of internet; merits and demerits of internet; various computer contaminants like virus, worms etc.

Emphasizing on the importance of computers and internet in day-to-day life they have expressed that Information Technology and ICT (Information Communication Technology) today have touched and influenced almost every aspect of our lives. We are in the era of information and computers are the main driving force. We do almost every activity that is some way or other dependent on computers.
They further suggested that now a days it is not sufficient that we need to be computer-literate, but we also need to understand the countless issues that are related to computers. He says further that there is relation between Human and Conflicts and law.

Commenting on the interlink of human conflicts and law, they states that where humans are, crime and conflict of interests cannot stay far behind. He further expresses that wherever crimes and conflict of interests are, law must come forward in order to control the situation. Thus, this paper have made a in depth study of the integral role of computer and internet and the cyber crimes –resultant of information technology.

Sharma (2010) in his book "Information Technology; Law and Practice" has evaluated the issues of jurisdiction in cyber space. While discussing the role of international law in deciding jurisdiction of cyber offences he has made references to various principles like nationality, passive personality, territorial, protective, universality, effects principle etc..Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals.28 Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length.

Chaubey (2009) in his book "An Introduction to Cyber Crime and Cyber Law" has emphasized on the significance of 'right to privacy' in digital age. He further states that the new technologies have improved the possibilities of interference into the privacy of individuals. Thus, individual privacy is at risk than ever before. Information Technologies like internet, computers can be used to store, deal and modify huge amount of data regarding people to violate privacy, confidentiality.

He has examined the concept of privacy in the light of various national and international laws. Further he explained that practices on internet which are common such as cookies, spamming that could lead to the breach of privacy. Also, he has highlighted the importance of adopting privacy policy by websites.

Dudeja (2002) in his book "Cyber Crime and the Law" has highlighted the relation of freedom of expression and the internet. He further said that few restrictions can be put on the use of ICT devices such as computers and Internet in the context of expression of freedom. This will be helpful for privacy and security of data of people and organisation. This is because now law identify Computer as a main tool of offence as well as a 'victim of crime'.

Ali (2016) in his paper titled “Determinants of preventing cyber crime: a survey research” has focussed the determinants factors for preventing cyber crime to the online business entrepreneur in Malaysia and Perak. These factors are Law Enforcement, Attitude, Awareness, Ethics and IT.

Singh (2010) in his book “Cyber Laws” has elaborately discussed the meaning and importance of intellectual property rights like trademarks, copyrights, patents etc. According to him, these rights refer to the property which is a creation of the mind e.g. inventions, art work, names, symbols, images, some designs used for business purpose.

Agarwal (2014) in his article on “Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements”, has stated that the law enforcement officials need to be trained on handling the new emerging cyber crimes and tackle them successfully.

He has suggested that there is need to set up a Cyber Crime Investigation training Cell in all the States of the country for giving training to the police officials, public prosecutors and judicial officers.

Behra, Abhimanyu (2014) in his article “Cyber Crime and Law in India”, has discussed various types of cyber crimes and also suggested strategies to curb them.

Dalal (2015) in his book “Jurisdiction in Cyberspace”, has elaborately examined the jurisdictional issue in trans-border cyber crimes and calls for an effective international regime to tackle the recently evolved cyber menace.

Nagpal, Rohasin (2005) in their article “Offences and Penalties under the Information Technology Act, 2000”, has made a critical study of various cyber crimes and corresponding penalties provided under the IT Act. He has also pointed out some loopholes in the Act and suggested measures to make it more effective.

Kotwal, Manhas (2017) in their paper titled “Investigation of different constraints in cyber crime and digital forensics” have taken the review of details regarding the growth of cyber crime and its various modes of occurrence at different level. This paper provides the understanding of various types of cyber crimes and its impact on different sections of the society.

Paranjape (2015) in his article “Cyber Crime: A Global Concern”, has focused on the global nature of cyber crimes and also presses the need for global measures to curb them.

Brown (2015) in his paper titled “Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice” has highlighted awareness regarding legal loopholes and enabling technologies, which facilitates acts of cyber crime. Author tries to identify factors which obstruct investigation, prosecution and digital forensics. Author further highlights that cyber criminals understands that technology is integral part of society. He emphasis that cyber is the prime global threat to national security.

Ramesh (2014) in his article “Pornography and Obscenity on the Web: Need a Strict Law”, has raised the issue of relevance of morality in cyber space by stating that obscene and pornographic contents in online mode has the tendency to spoil innocent young minds.

Sharma (2012) in his article “Globalization and its Impact on Cyber Crime: Case Study of Indian Police Administration”, has examined the impact of globalization, liberalization and privatization on the cyber crimes and concluded that more advancement in technology leads to highly technical nature of the crimes.

Perry4law which is a Corporate in Techno legal domain is a firm of IP & ICT Law of India. It writes about “Cyber Forensics” in the article (2014) that India needs to strengthen. He further says that Cyber Forensics and Cyber crime investigation improvements in India needs to improved and strengthened.

In this article, experts say that in India, the investigation in the domain of Cyber Forensic investigation needs to be developed in a better manner. The experts also adds that India do not have “Cyber Forensics Best Practices”. Cyber Forensics is conducted in a casual manner. Digital evidence and scientific approach for investigation is still lacking in Legal system as well as Judicial system of India.

Perry4law (2013) in their one of the Blogs emphasis on special attention to cyber forensics best practices in India. According to some experts issues of importance as follows:

1) Techno Legal skills developments in India need to be achieved.
2) Computer Forensics training in India is urgently required.
3) Education Institutes along with basic level course must insist more skill oriented 'Cyber Forensics' and 'Information Technology' courses.
4) Law Enforcement Agencies of India are not well equipped to deal with the most basic cyber crimes.
5) Police Officers in India need to be trained in the fields of cyber crimes investigation.
6) Forensics companies and websites are not complying with Indian Laws.
7) Registration of FIRs by Police is must.

PTLB (2014) emphasis on urgent need to form an effective Technical and legal Framework. This will help to deal with issues related to techno legal aspects of cyber crime.

They further highlight that in many incidences of cyber crimes in India, Law enforcement bodies or agencies have not conducted proper discovery of evidences and cyber forensic cases. This has made their cases weak. Accused due to this may escape the punishment.

2.4 Gaps identified from Literature review

After reviewing literature of various National and International reports, Policies, Expert's Articles, Books on cyber crimes following gaps have been identified to make our country and society Cyber safe.The literature review reveals that there is a great need to undertake a systematic study of factors affecting effective investigation of cyber crimes.

1. Cyber criminals continue to take advantage of vulnerabilities in authenticate or legitimate websites. Their objective is to infect users. This happens because administrators of websites fail to secure customer's websites.

2. Cyber criminals are using Encryption as a weapon to hold companies' and individual's critical data.
3. Many scams still depend on the weak security habits of the common people to proceed. However if website security is not strengthened, customer data can be exposed to cyber attackers.
4. Scams related to Social networking need some form of interaction and manual sharing. This was the main reasons of social media attacks. With increased digitization, people are sharing their personal data more than ever.
5. Organisations showed lack of security system to identify fake, illegitimate mails through company's mail server.
6. Attackers are shifting towards cyber attacks that give them huge amount of money in an easier way. Ransomware campaigns have higher returns compared with other data stealing campaigns.
7. People were prudent enough to keep their Operating Systems up-to-date
8. Phishing crimes are increasing. Defences though are improving, are not still sufficient.
9. Awareness is being recognized as an important factor in the strategy to tackle cyber threats.It has been found that there is a lack of awareness amongst people of different age groups on cyber safety. People don't know simple do's and don'ts about cyber crimes.
10. Many people or Employees in the organisation are not aware of ransomware and their important role in protecting the organization's data.
11. Need to configure mechanisms of access controls, including file, directory, and different types of networking to share permissions appropriately. If users only need specific information that reads data only, they don't need the permission of write-access to those files or directories.
12. People do not take data Backup regularly.
13. Need to draft the cyber security policy of India. The security policy of the 2013 is highly defective.
14. Intelligence Infrastructure of India needs to be built. It requires transparency. To make it "Effective and Accountable" it needs to be strengthened.

15. It has been found that companies are doing investment on technology. But they are not investing on training to people about cyber threats.
16. There is a gap found on providing additional security layer to security products and services. e.g. use of firewall.
17. It has been found that cyber attackers are not caught. This has increased risk of cyber attacks and cyber crimes. It is not easy to catch cyber attacker as cyber attackers maintain anonymity
18. Smart cities have been found less cyber secure due to increased use of Mobile, Internet, computers etc.
19. Most of the organizations such as Educational, financial and technology institutes have not drafted the cyber security policy.
20. In India, we miss proper Infrastructure or framework for cyber security.
21. Police officers are not trained to collect electronic evidence from the computers which need to be presented in the court. There are immense problems of proofs in cyber offences to present in the court.

After reviewing various National and International reports, the present research is focused on ‘Cyber crimes in Pune, India’. Year 2011-2016 were considered for the study of cyber crimes in India as the rate and percentage of cyber crimes are increasing every year. The cyber crimes resolved and Pending are inverse in proportion which is the reason of study of present research.

CHAPTER 3- RESEARCH METHODOLOGY

This Chapter is discussed under the following headings

3.1- Introduction

3.2- Research Questions

3.3- Objectives of the study

3.4- Statement of Hypothesis

3.5- Design of the Questionnaire

3.6- Pilot study

3.7- Selection of Sample

3.8- Collection of Data

3.9- Analysis of Data

3.10- Statistical Tools used for Analysis of Data

3.11- Limitations of the study

3.1 Introduction

Use of Internet and Information Technology along with new advancement has given birth to different types of Cyber Crimes.

The researcher has chosen this topic to study the gaps in investigation of cyber crimes which with given proper solutions can be minimized. Improvisation in investigation process and speedy investigation can minimize the rate of rising cyber crimes.

Revision of existing cyber crime investigation process will minimize the investigation time which will help society from cyber terrorism.

In order to come up with detailed analysis on the gap areas, the researcher has attempted to do in-depth study on various aspects of 'Life cycle' of cyber crime investigation process.

Data of Cyber crimes from various Cyber Cells of Maharashtra was collected via Questionnaire through RTI (Right To Information Act).

Besides, responses of people in Pune city between age group of 18-30 years based on their 'Cyber Safety Awareness' were collected via a Questionnaire.

Cyber Crime statistics of Pune City and PCMC area was collected through all 39 police stations via a Questionnaire through RTI (Right To Information Act).

Responses of the DCP/ACP from various police stations in Pune City and PCMC area were collected via a Questionnaire.

3.2 Research Questions

After review of literature related to cyber crimes, some research questions are framed as follows:

1) Why there is no control on increase of cyber crimes in India?
2) Why there is inverse proportion of cases registered and persons arrested under cyber crimes?

3) Why certain states have highest no. of crimes?
4) Why there is rise in cyber crimes in some cities in last 3 years?
5) Why cyber crimes of particular type are increasing in society?
6) What is the motive behind cyber crimes?
7) What are the social, legal, technical aspects and obstacles in investigation of cyber crimes?

3.3 Objectives of the Study

The main purpose of this study is to find out why there is gap between number of cyber crimes registered and number of cyber crimes resolved, why many cyber crimes investigations are pending or cases not resolved.

The proposed study will attempt to address the following objectives in order to contribute to the investigation process which will help various Police Stations, Cyber Cells, Cyber Forensic Labs and Cyber Crime Investigators.

Objectives:

1. To find out 'Cyber safety Awareness' amongst people of age group of 18-30 years and above 30 years.
2. To find out the crimes registered, investigated and pending with reasons in all Cyber Cells of all Police stations of Pune city.
3. To find out factors affecting effective investigation of cyber crimes in Pune region from experts in this area.
4. To impart training to school children of age below 18 years so that they will be more aware on cyber safety and cyber crimes.
5. To propose a model for cyber crime investigation process that will help all Cyber cells, Cyber Forensic Lab and Police stations of Maharashtra for timely investigation of cyber crimes.

The outcome of this study will help to improve success rate of cyber crime investigation process and decrease rate of cyber crimes in society.

3. 4 Statement of Hypothesis

For the present study following **Alternate and Null** Hypotheses were formulated.

(Please Note: - H_1 is Alternate and H_0 is Null Hypothesis)

Hypotheses Statements:

1) **Hypothesis 1:**

   H_1 --There is a significant difference in the **cyber safety awareness** between age group of 18-30 years and above 30 years.

   H_0 -- There is not a significant difference in the **cyber safety awareness** between age group of 18-30 years and above 30 years.

2) **Hypothesis 2:**

   H_1– There is an association between various aspects of ICT which leads to the cyber crimes.

   H_0– There is no association between various aspects of ICT which leads to the cyber crimes.

3) **Hypothesis 3:**

   H_1 --Cybercrime investigation has affected the Pune commissionerate due to the manpower available with the police stations for cybercrime investigation is in appropriate.

   H_0 --Cybercrime investigation has not affected the Pune commissionerate due to the manpower available with the police stations for cybercrime investigation is appropriate

4) **Hypothesis 4:**

   H_1-- There is an association between training provided to staff and problems faced while investigation of cyber crimes.

   H_0 -- There is no association between training provided to staff and problems faced while investigation of cyber crimes.

5) **Hypothesis 5:**

H1 -- Cyber criminals are on rise since the number of crimes related to cyber security has not been resolved.

H0: Cyber criminals are not on rise since the number of crimes in related to cyber **s**ecurity has not been resolved.

This kind of research study is unique as it is not done or published anywhere as per the search on online or offline sources. This research will help the Cyber Cell of Pune and various police stations in Pune city.

3.5 Design of the Questionnaire

The 'Questionnaire Method' was adapted for collection of data for the present study. 5sets of questionnaires were prepared for collecting data from different sets of people.

Questionnaire-1 was filled by officials/personnel from various Cyber cells and Cyber Forensic Lab of Maharashtra for the year 2009-2011.
Questionnaire-2 was filled by the 1122 people of age-group 18-30 years on 'Cyber Safety Awareness'.
Questionnaire-3 was filled by Cyber Cell- Commissioner Office, Pune and all Police stations in Pune city and PCMC area where cyber crimes are registered.
Questionnaire-4 was filled by ACPs of various Divisions of police stations on 'Problems faced by police stations on cyber-crime Investigation'. **Questionnaire -5** was filled by 54 Principals of schools in Pune.

Questionnaires were designed to study different angles of cyber crime investigation such as frequent cyber crimes, reasons of pending cases, user behavior while using Internet, Online Banking and other e-transactions, Email, legal aspects etc.
The records of last five years (2011-2016) were collected from various police stations, Cyber Cells in Tabular Format.

Questionnaires were prepared to understand problems faced by Cyber Cells, Police stations in investigation of cyber crime. It was filled by ACP/DCPs of various Divisions of Police stations in Pune city.

1. Defining Target Respondents :

The sets of respondents were selected. They were

1) Assistant Police Inspectors

   All 39 police stations in Pune and PCMC were selected for the research. In every Police station, there is an API who handles the cyber crime issues.
2) Internet Users (age group 18-30 and above 30 years)
3) DCP/ACP from Police stations
4) Cyber cell, Pune
5) Cyber Crime Investigation Officers

2. Choosing the method (s) of reaching to the target respondents :

To reach the target respondents, the method chosen was the Questionnaire and Interview.

As the Cyber Cell, Cyber Forensic Lab and all police stations come under Maharashtra Government, information via Questionnaire was obtained through Right to Information Act (RTI) which helped to get authentic information from these sources. Apart from RTI, various respondents were followed up through telephone, Personal Interview by visiting Cyber cell and all Police stations.

3. Deciding on Question content :

a. Questionnaire to be filled by various police stations was prepared under the guidance of ACP of Cyber cell and Cyber Forensic Lab- Pune and Research guide.

b. Questionnaire format for collecting Cyber Crimes Statistics was given in simple Tabular Format.

c. Questionnaire format for collecting data on awareness of Internet users on cyber safety was in Objective and in Yes/No Format for ease of filling data.

4. **Deciding the question wording :**

   The wording of the questions was kept simple so that respondents could easily understand and respond.

3.6 Pilot Study

While designing questionnaire, expert guidance of ACP of Cyber Cell, Pune and Cyber crime Investigation Officer was taken. He reviewed trial questionnaire which was edited after making it more comprehensive, compact, meaningful and purposeful based on their experience in the area. Guidance of Research Guide was taken for sequence, order of questions, reference etc.

Based on the suggestions and inputs received by the various respondents, the final Questionnaires and Hypotheses were formulated. The samples of Final questionnaires are attached in Appendix Section.

The sets of respondents were identified. They were :

Respondent1:Asst. Police Inspector (API) and Deputy Commissioner of Police (DCP) from Santa Cruz, Thane, Mumbai, Pune Cyber Cells

Questionnaire 1 was formed to get information of cyber crime scenario in Maharashtra State. The above respondents were communicated via RTI application form.

Respondent 2:People of age group 18-30 years and above 30 years

Questionnaire 2 was formed with a view to obtain Cyber safety awareness of people. For this, a sample of 1122 people was selected. They were selected from all backgrounds such as people from Education background (Students, teachers), Industry people and Senior citizens etc.

Respondent 3:Senior Police Officers from Pune and PCMC Police stations

Questionnaire 3 was formed to collect data from all 39 police stations of Pune and PCMC and Commissioner Office of Pune. In every Police station there is an API who handles the cyber crime issues.

Respondent 4:DCP and Senior Police Officers from Pune and PCMC Police stations

To study the problems faced by Cyber cells and Police stations for investigation of Cyber crimes, Questionnaire 4 was prepared and data collected from all 39 police stations of Pune and PCMC as well as from Cyber Cell -Commissioner office, Pune.

Respondent 5:Principals/Coordinators of 54 Secondary Schools (Std. V-X) of Pune and PCMC area

Need of 'Cyber Safety Awareness Campaign' in students of age group of 11-16 years was identified. To do this, Questionnaire 5 was administered to the Principals/ coordinators of 54 Secondary schools of Pune and PCMC area.

3.7 Selection of Sample

After finalization of the questionnaires, the researcher started approaching various respondents like Cyber Cell-Pune, all Police stations in Pune city and PCMC area and people of age group of 18-30 years and above 30 years.

Questionnaire-1 was responded by API, Police Commissioner of various Cyber cells and Cyber Forensic Lab of Maharashtra for the year 2009-2011. Information was obtained through RTI from 5 cyber cells and cyber Forensic labs. The data from Pune, Mumbai, Thane, and Santa Cruz –Cyber Forensic lab were selected to get a view of cyber crimes scenario of Maharashtra. (Appendix-1)

Questionnaire-2 on '**Cyber Safety Awareness'** distributed to 1122people of age group 18-30 years and above 30 years in various conferences, seminars and colleges. Total 1122respondents responded to Questionnaire-2. Data was collected in hard copy format. This data was then converted into online Google's utility-**Google Form**, which was easier for compiling and analyzing data in required formats like Excel format, graphs etc. This data was then processed through SPSS 23. The Findings of this analysis are discussed in Chapter 4.

Questionnaire-3 was on **'Cyber Crime Statistics (2011-16)'** was distributed to various Police stations (39) in Pune city and Cyber Cell, Pune through Right To Information (RTI) Act.ar It was responded well by the API and cyber crime investigation officers. Out of 39 Police stations,34 Police stations have given the information after the researcher's personal visit and via Post.

Questionnaire-4 was on **'Problems faced by police stations on cyber-crime Investigation'.**

This was filled by ACPs of 10 Divisions of police stations. The information was obtained in person through visit to Police station and meeting with them.

Questionnaire-5 was designed for School Principals to get their feedback on need of 'Cyber Safety Awareness' for school children below 18 years.

All these questionnaires helped the researcher to obtain authentic and reliable information which helped to progress further on the research study.

The Sample of the study bears the following characteristics.

1) Different respondents related to cyber-crime and crime investigations such as Internet users of age group (18-30 years), ACP/DCPs of cyber cell & police stations in Pune city, Cyber Lawyers and ethical Hackers were involved. This helped to get 360 degree feedback from people related to cyber-crime and its investigation.
2) The details obtained from them are based on their experience and actual cyber-crime statistics available in Police stations in last 5 years (2011-16).

The regions of Pune City and PCMC were considered for this study.

3.8 Collection of Data

Primary data :

Primary Data is firsthand information collected through various methods such as Questionnaire, Observation, Interview, e-mailing etc. Primary Data is directly collected by the researcher from their original sources. The researcher has collected the required data precisely according to research needs.

For the present study, the primary data was collected as follows :

1) **Questionnaire1**: Cyber cells and Cyber Forensic labs in Maharashtra
   Sample size:5
   Data Collection method: Questionnaire through Right to Information Act (RTI)
2) **Questionnaire 2**: People of age group 18-30 years and above 30 years
   Sample size: 1122
   Data Collection method: Questionnaire
3) **Questionnaire3**: Police stations in Pune city, PCMC area and Cyber Cell, Crime Branch : Pune
   Sample size: 39
   Data Collection method: Questionnaire through Right to Information Act (RTI) and Personal visit to each Department
4) **Questionnaire4**: 39 Police stations from Divisions of Pune and PCMC
   Sample size: 10
   Data Collection method: Questionnaire through Right to Information Act (RTI) and Personal visit to each Department
5) **Questionnaire5**: School Children of Pune city below 18 years of age
   Sample size: 54 schools
   Data Collection method: Form

Secondary data:

Secondary data was collected from various online and offline sources.

Reports from Government‘s official Websites, Information security Company’s Websites were studied.

Articles from Journals, e -Journals, Magazines, Newspapers, Reference books and Text books on cyber crimes and information security were reviewed. Besides this, various books on cyber laws were referred.

3.9 Analysis of Data

1) The data collected has been tabulated and presented in the form of tables, charts and graphs.

2) The Karl Pearson’s correlation coefficient test was applied to the variables of the quantitative data and the correlation between +ve and –ve variables were established. Details of the same are given in Appendix.

3) Descriptive data was formulated in tables and was analyzed for results and outcomes.

4) Each question of the questionnaire was tabulated w.r.t. Likert scale and descriptive analysis like mean, median etc.

5) Line Graphs, Pie Charts, Bar Graphs were generated to see the behavior of the data collected against the total sample:

   n=5 for Questionnaire-1

   n=1122 valid response of people of different age groups for Questionnaire-2

   n=39 police stations for Questionnaire 3

   n=10 for Questionnaire 4

   n=76 schools for Questionnaire 5

6) Hypotheses were tested using SPSS -23 software for statistical analysis.

Data Collection and Analysis Flow Chart

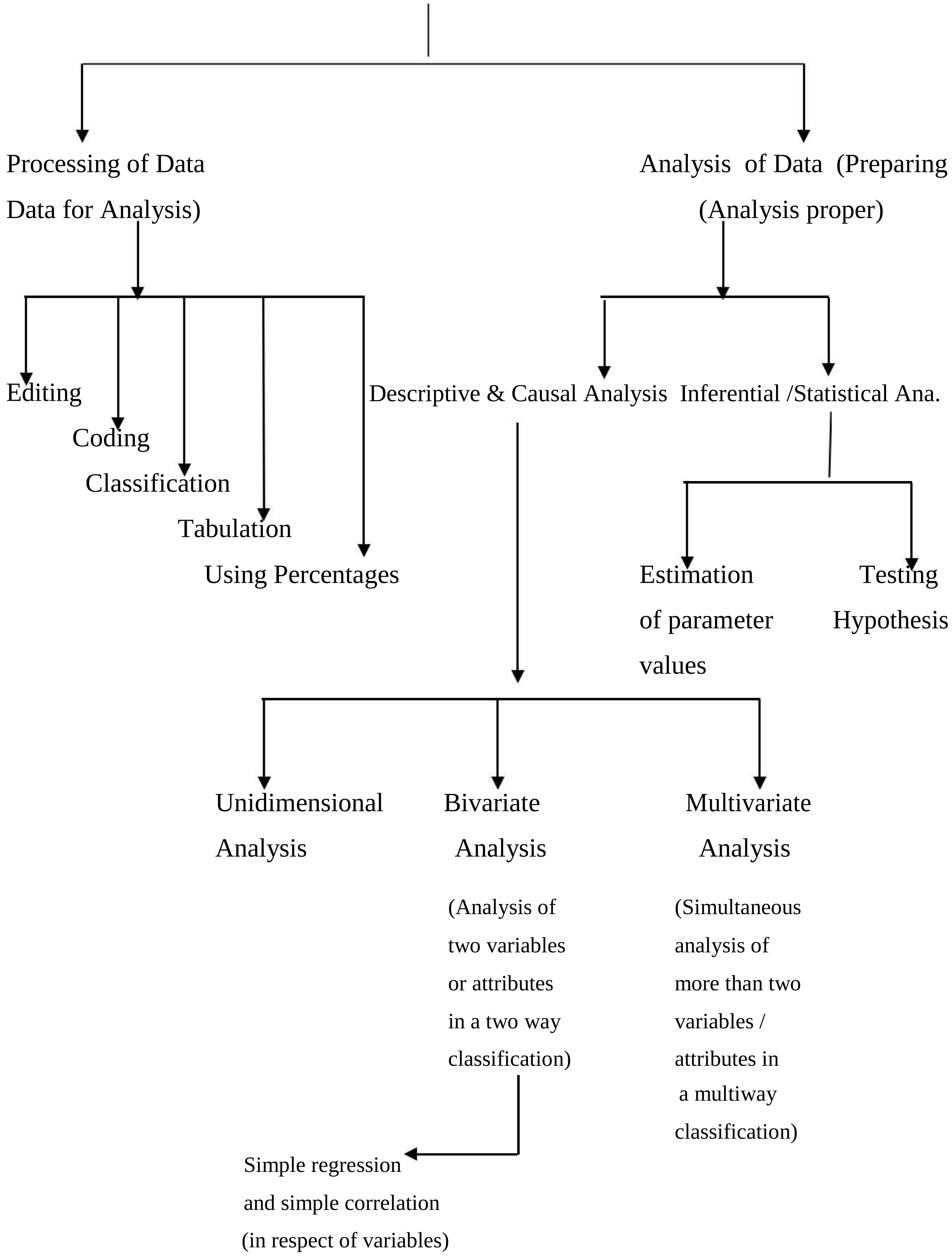


Figure 1: Data Collection and Analysis Flow Chart

3.11 Limitations of the Study

1 Through the exhaustive Review of Literature, particularly through the reports of NCRB (National Crime Records Bureau of India), the researcher learnt that the state with the highest cyber crimes is Maharashtra. Hence, to get an overview of cyber crimes in the state of Maharashtra, major cyber cells in Pune, Mumbai, Thane and Santa Cruz were approached.

2 It was found that the most frequently committed cyber crimes are registered under Section 65, Section 66 (A-E) and Section 67 of the Information Technology Act 2000.Hence, only the cyber crimes under the above sections were studied.

3 As the research study was focused on the researcher's place of residence i.e., Pune city; the police stations in Pune and PCMC area were considered for the study.

4 The researcher learnt that there are a total of 39 police stations in Pune and PCMC area. All 39 were approached, out of which only 34 police stations furnished the required information. The remaining 05 police stations either not given or denied the information.

`

CHAPTER 4 – RESULTS AND ANALYSIS

This chapter is discussed under the following headings

4.1 –Research Strategy – Steps of the Research Process

4.2 - The Cyber crime Scenario in various states of India (2009-2015)

4.3 – Best Practices of other countries for cyber security

4.4 - The Cyber Crime Scenario in Maharashtra (2009-2011) [through RTI]

4.4.1 Organisational Structure of Cyber Crime Investigation

4.4.2 Study of report given by Cyber Forensic lab, Santa Cruz (Mumbai), Maharashtra state (Dt. 7.11.12)

4.4.3 Study of cyber crime report given by cyber cell, crime branch, Thane, Maharashtra state (Dt. 22.11.12)

4.4.4 Study of Report Given By Cyber Cell, Crime Branch, Mumbai Dt.26/11/2012

4.4.5 Study of report given by cyber cell, crime branch, Pune Dt. 5/12/2012

4.5– Analysis of Cyber crime scenario in Pune City [through RTI]

4.6 –Analysis of Cyber safety Awareness amongst Internet users in Pune city

4.7 –Analysis of the Problems faced by Cyber Cells, Police stations in Pune city during cyber crime Investigation Process [Questionnaire 4 through RTI and Interview process]

4.8 –Identification of Need of Cyber Safety Awareness for school children below age Group of 18 years

4.9 –Cyber Security Risk Assessment Matrix based on results of 4.2 - 4.8

4.10 --Hypothesis Testing

`

4.1 Research Strategy:

Research related to Cyber crimes is carried out as follows:

The methods adopted to get research related information are Questionnaire, field visits, Interview, record reviews at field location etc. Most of the information was collected through Right To Information Act (RTI Act).

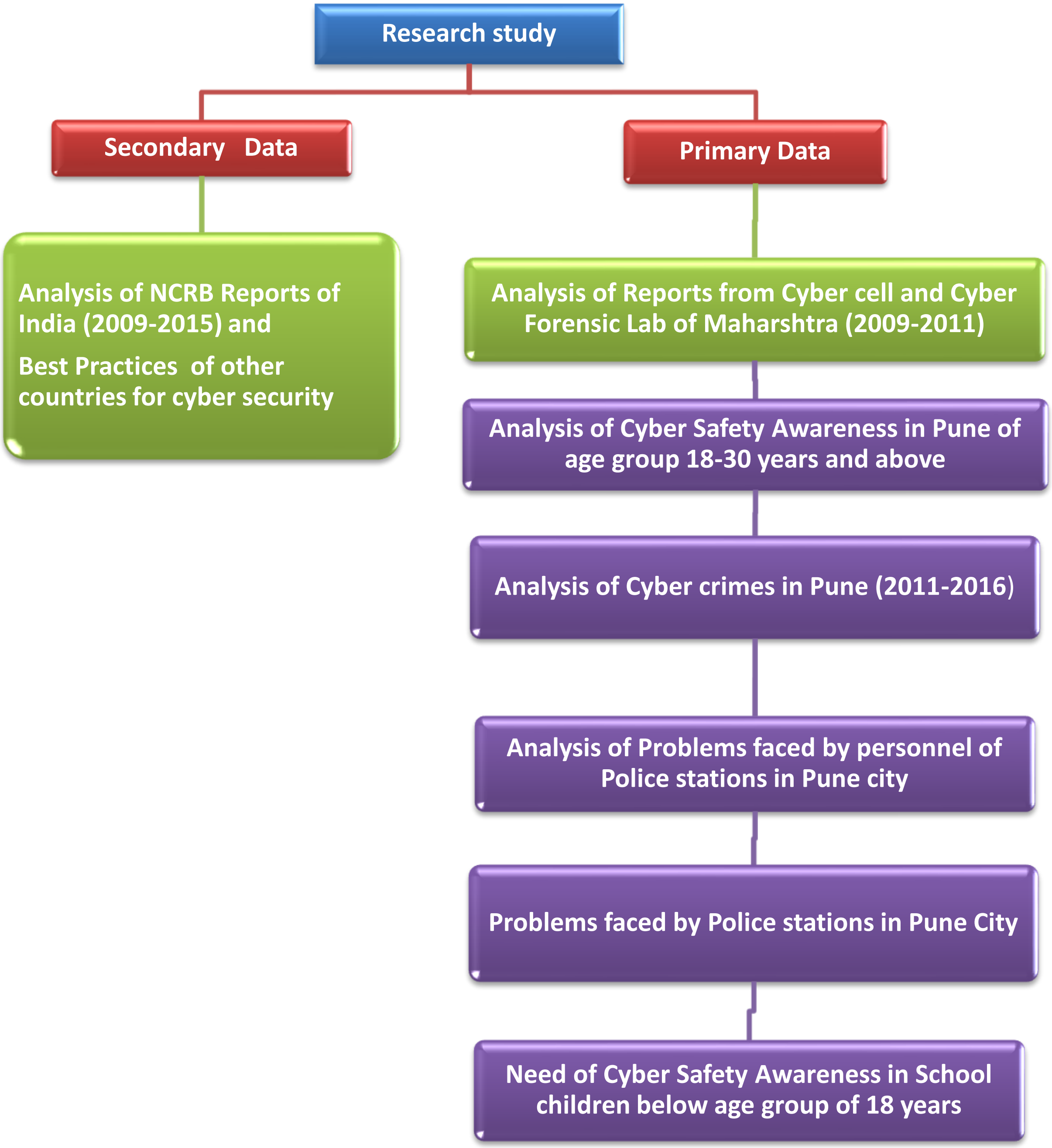

Research study
Secondary Data
Primary Data
Analysis of NCRB Reports of India (2009-2015) and
Best Practices of other countries for cyber security
Analysis of Reports from Cyber cell and Cyber Forensic Lab of Maharshtra (2009-2011)
Analysis of Cyber Safety Awareness in Pune of age group 18-30 years and above
Analysis of Cyber crimes in Pune (2011-2016)
Analysis of Problems faced by personnel of Police stations in Pune city
Problems faced by Police stations in Pune City
Need of Cyber Safety Awareness in School children below age group of 18 years

Figure 2: Steps of the Research Process

`

4.2 - The Cyber Crime Scenario in Various States of India (2009-2015)

Cyber Crime status of various states of India (year 2009-2015) have been studied to get the trend of cyber crime, the highest number of cyber crimes committed year wise and state wise. Reports of National Crime Records Bureau of India (NCRB) from year 2009 -2015 have been studied for this as follows:

1) Incidences of cases registered under cyber crimes in Selected States of India (2009-2015)
2) Persons arrested under cyber crimes in Selected States of India (2009-2015)
3) City wise Cases registered of Cyber crimes in Selected Cities of India(2009-2013)
4) Cyber crimes registered of Cyber crimes in selected cities of Maharashtra (2009-2013)
5) Persons arrested under IT Act in States By Age Group Below 18 years (2009-13)
6) Persons arrested under IT Act in States By Age Group Between18-30 years (2009-13)
7) Persons arrested under IT Act in States By Age Group Between 30-45 (2009-2013)
8) Incidences of Total cases registered and persons arrested under Cyber crimes (IT Act) during 2009-13 (All India)
9) Disposal of Cyber Crime Cases (IT Act) by Police during 2014-2015

`

Table 4: Incidences of cases registered under cyber crimes in Selected States of India (2009-2015)

Sr. No.	Selected States of India	2009	2010	2011	2012	2013	2014	2015	Total
1	Maharashtra	53	142	306	471	907	1879	2195	**5953**
2	Uttar Pradesh	14	32	101	205	682	1737	2208	**4979**
3	Karnataka	97	153	151	412	533	1020	1447	**3813**
4	Rajasthan	27	52	122	147	297	697	949	**2291**
5	Andhra Pradesh	30	105	349	429	282	282	536	**2013**
6	Kerala	64	148	227	269	383	450	290	**1831**
7	Telangana	0	0	50	0	150	703	687	**1590**
8	Madhya Pradesh	16	30	90	142	342	289	231	**1140**
9	Punjab	28	41	59	72	156	226	149	**731**
10	Gujarat	20	35	52	68	77	227	242	**721**
11	Tamil Nadu	18	52	37	39	90	172	142	**550**
12	Goa	8	15	16	30	58	62	17	**206**
	Total	**375**	**805**	**1560**	**2284**	**3957**	**7744**	**9093**	

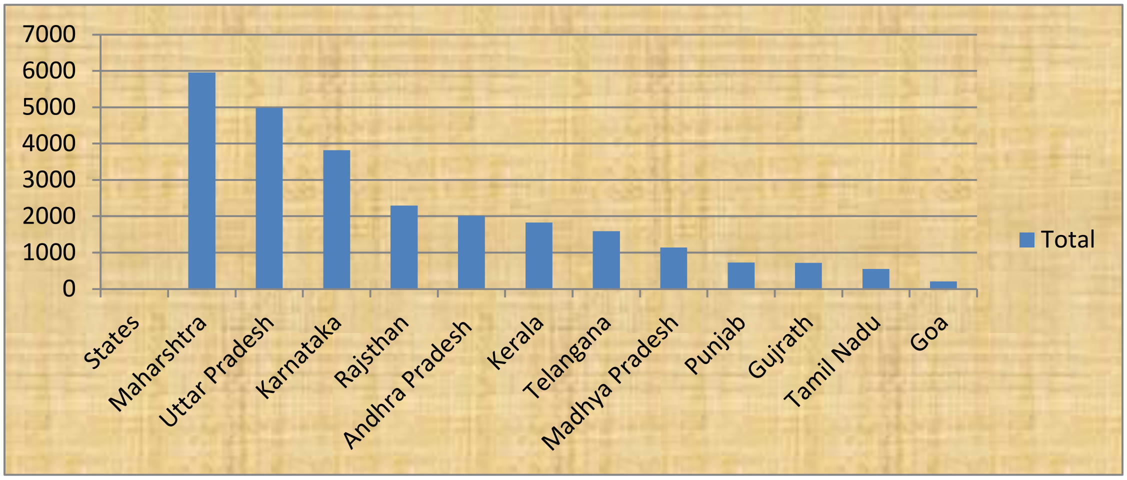


Figure 3: Total Cyber crimes registered in Selected states of India (2009-2015)

INFERENCE: Figure 3 highlights the following facts on cyber-crimes.

1) Maharashtra, Uttar Pradesh, Karnataka and Rajasthan show highest number of cyber crimes committed in the last 7 years(2009-2015) compared to other states. The situation of cyber crimes is alarming in these states and the rate of cyber crimes is increasing drastically.
2) As compared to 2009 and 2010, cyber crimes have started increasing from 2011.

3) Of all the above states, Maharashtra is showing highest number of cyber crimes (5953) in India which is of serious concern.
4) Rise in Cyber Crimes in these states are indicative that cybercrime is spreading all over India slowly and there is need of great control to minimize and stop it.

Table 5: Persons arrested under cyber crimes in Selected States of India (2009-2015)

Sr.No.	**States**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**Total**
1	Maharashtra	10	88	140	215	603	942	825	**2823**
2	Uttar Pradesh	15	40	52	60	602	1223	1699	**3691**
3	Karnataka	9	56	30	35	104	372	293	**899**
4	Rajasthan	20	21	71	55	133	159	136	**595**
5	Andhra Pradesh	6	25	142	125	313	236	522	**1369**
6	Kerala	25	61	86	81	169	283	191	**896**
7	Telangana	NA	NA	NA	NA	41	56	53	**150**
8	Madhya Pradesh	20	27	63	105	177	386	230	**1008**
9	Punjab	12	15	25	22	133	159	136	**502**
10	Gujarat	9	24	17	41	65	174	272	**602**
11	Tamil Nadu	5	28	18	20	97	120	125	**413**
12	Goa	0	1	4	3	11	14	5	**38**
	Total	**131**	**386**	**648**	**762**	**2448**	**4124**	**4487**	

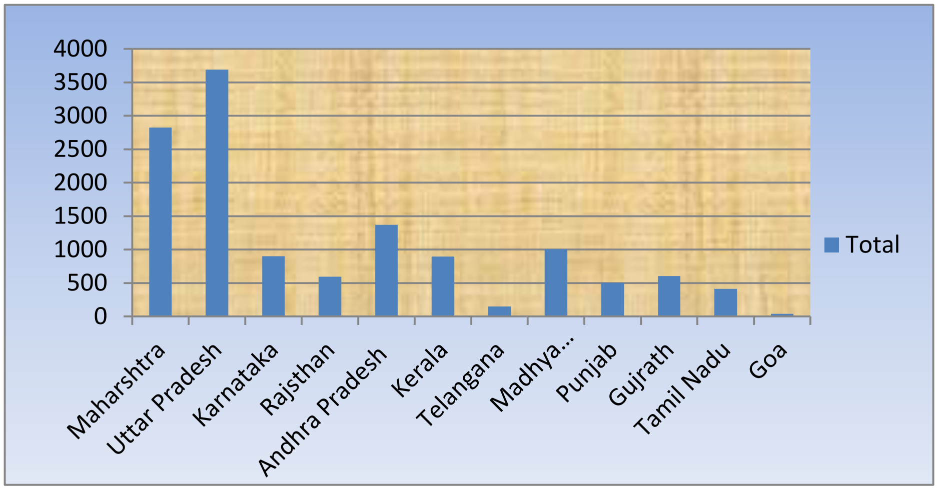


Figure 4 : Total Persons Arrested under Cyber Crimes in Selected States of India (2009-2015)

`

INFERENCE: Figure 4 above highlights the following facts on cyber crimes:

1) Maharashtra and Uttar Pradesh show the highest numbers of persons arrested as compared to other states.
2) Persons arrested in these states are very less as compared to Cases registered. e.g., in Maharashtra, cases registered are 5953 and in Uttar Pradesh they are 979 whereas persons arrested in these states are only 2823 and 3691 respectively i.e. 47% and 74% respectively. This gives space for Cyber criminals to commit more cyber crimes as they are not arrested.

Table 6: City wise Cases registered of Cyber crimes in Selected Cities of India (2009-2013)
***[Green Shaded area shows Top 5 cities of India. Yellow Shaded areas shows cities of Maharashtra]**

S.No.	**City**	**2009**	**2010**	**2011**	**2012**	**2013**	**Total**
1	Hyderabad	0	51	67	42	159	**319**
2	Bengaluru	97	40	117	342	399	**995**
3	Pune	5	32	83	76	97	**293**
4	Jaipur	0	27	76	69	110	**282**
5	Delhi	5	41	50	73	131	**300**
6	Kochi	6	3	29	45	26	**109**
7	Kolkata	0	3	6	68	84	**161**
8	Aurangabad			19	31	47	**97**
9	Ahmedabad	10	8	24	25	24	**91**
10	Lucknow	0	0	20	23	37	**80**
11	Mumbai	4	8	8	33	40	**93**
12	Nagpur	2	5	11	24	23	**65**
13	Chennai	2	10	13	15	5	**45**
14	Vadodara	3	10	14	14	13	**54**
15	Coimbatore	6	12	15	3	3	**39**
16	Nasik	4	14	2	11	18	**49**
17	Indore	5	5	6	5	28	**49**
18	Allahabad	4	1	5	4	17	**31**
19	Bhopal	6	10	5	1	19	**41**
20	Varanasi	0	11	4	2	6	**23**

`

Why are Cyber crimes high in a few Cities?

From the above table, one can observe that Cyber crimes in cities like Hyderabad, Bengaluru, Pune, Jaipur, Delhi are highest compared to other cities. We know that these are **Capital cities** of Andhra Pradesh, Karnataka, Maharashtra, Rajasthan, Uttar Pradesh, respectively. These states have good *geographical, educational, political and cultural heritage* which gives conducive environment for overall growth of Economy, Technology, Science, Fashion etc.. Most of these cities are declared as IT hub in last 10 years. This has further mobilized the technological development to great extent. Development of various Universities for education attracted younger generation from India and abroad. Due to affordability of Internet and mobile in all strata of society, use of technology by younger generation has been motivated which also motivated the crimes over the internet /mobile known as cyber crimes.

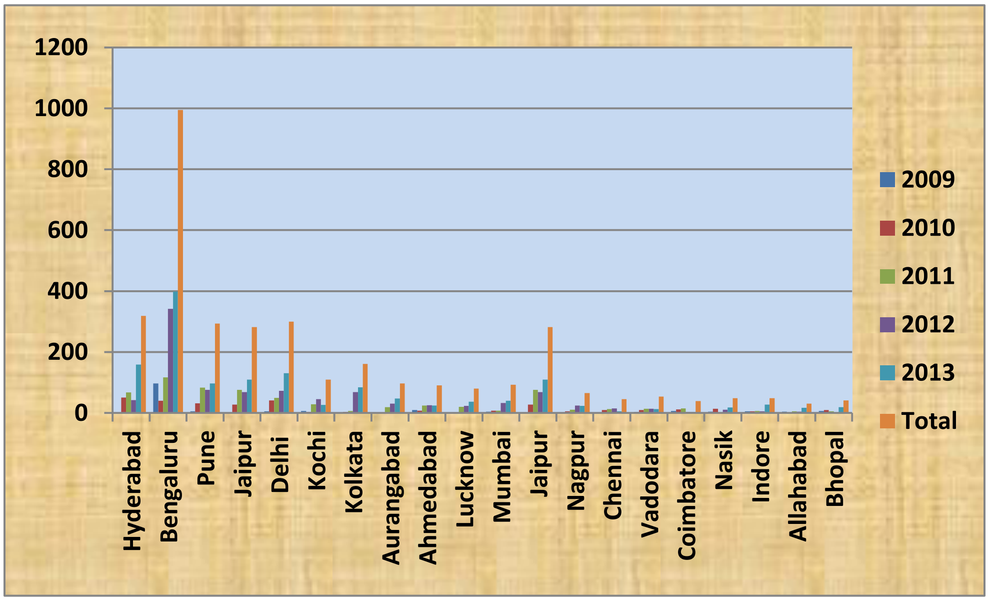


Figure 5: City wise cyber crime cases registered in selected cities of India (2009-2013)

INFERENCE:

Figure 5 highlights the following facts on cyber crimes:

1) Bangalore has highest number of cyber crimes registered in India from 2009-2013.The crimes are increasing significantly from 2009-2013.

`

2) Hyderabad, Delhi, Pune and Jaipur have greater numbers of cyber crimes from 2009 to 2013 respectively. Numbers of cyber crimes are notable in these cities.
3) Cities of Maharashtra –Pune, Aurangabad, Mumbai, Nagpur, and Nasik have highest number of cyber crimes committed in these years.
4) Of all the cities of Maharashtra, Pune shows highest number of cyber crimes.

This alarming inference compelled the researcher to study cyber crimes in Pune city for research. A systematic study of cases registered, persons arrested under IT act in these major cities of Maharashtra are carried out.

Table 7: Cyber crimes registered in selected cities of Maharashtra (2009-2013)

Sr. No	**City**	**2009**	**2010**	**2011**	**2012**	**2013**	**Total**
1	Pune	5	32	83	76	97	**293**
2	Aurangabad	0	0	19	31	47	**97**
3	Mumbai	4	8	8	33	40	**93**
4	Nagpur	2	5	11	24	23	**65**
5	Nasik	4	14	2	11	18	**49**

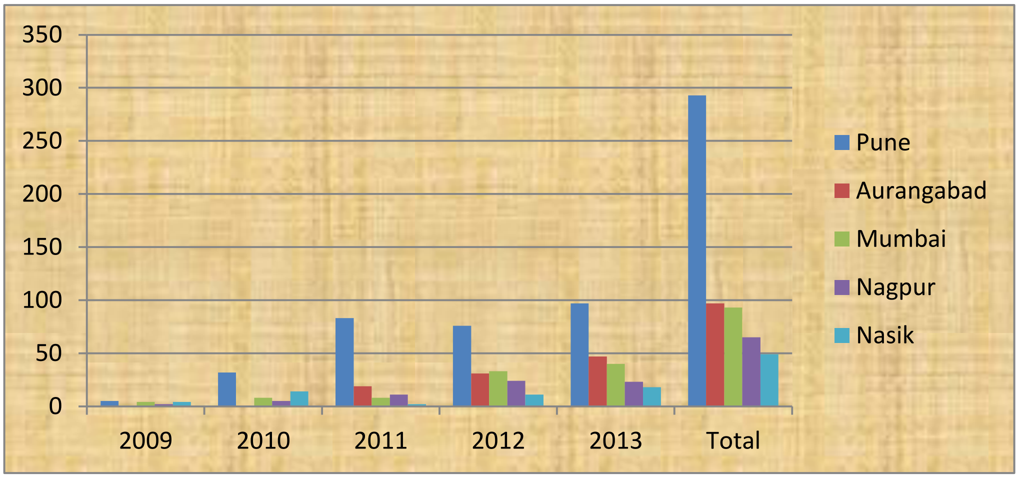


Figure 6: Cyber crimes Registered in selected cities of Maharashtra (2009-2013)

INFERENCE: Figure 6 highlights the following facts on cyber crimes:

1) In Maharashtra, Pune city shows the highest number of cyber crimes which is approximately 3 times greater than Mumbai.
2) Cities like Pune, Aurangabad, Mumbai, Nagpur and Nasik have importance as crimes committed in these cities are of utmost importance. These are developing and promising Smart Cities of Maharashtra.

Table 8: Persons arrested under IT Act in States by Age Group Below 18 years (2009-13)

Sr.No.	States	2009	2010	2011	2012	2013	Total
1	Maharashtra	6	5	4	9	17	**41**
2	Uttar Pradesh	0	7	0	0	0	**7**
3	Karnataka	0	2	0	3	0	**5**
4	Rajasthan	0	0	1	13	2	**16**
5	Andhra Pradesh	0	0	5	0	9	**14**
6	Kerala	4	1	3	15	9	**32**
7	Madhya Pradesh	0	1	10	13	2	**26**
8	Punjab	0	0	0	0	4	**4**
9	Gujarat	0	0	0	1	0	**1**
10	Tamil Nadu	0	0	0	1	0	**1**
11	Goa	0	0	0	1	0	**1**
	Total	**10**	**16**	**23**	**56**	**43**	

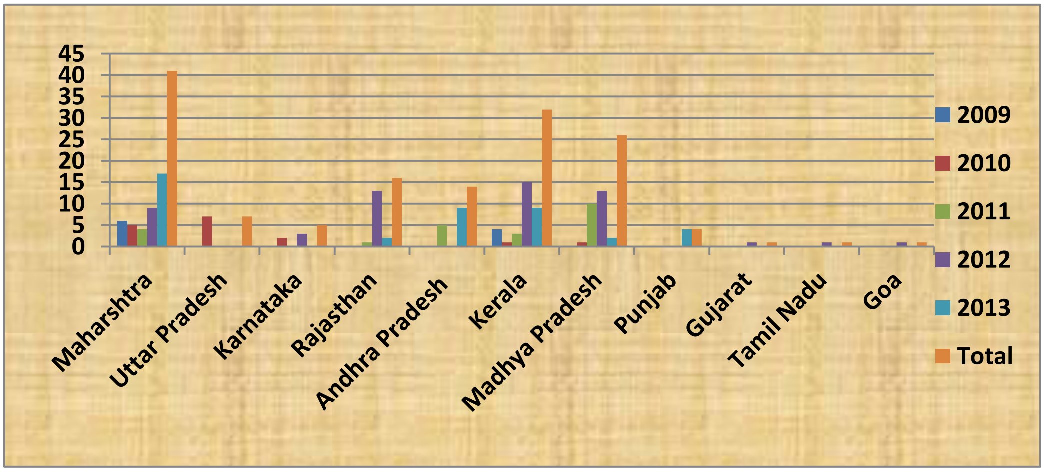


Figure 7 : Persons arrested under IT Act in States By Age Group Below 18 years (2009-13)

INFERENCE: Figure 7 highlights the following facts on cyber crimes:

Cities where crime rate is higher is studied with reference to different age groups.

1) Persons arrested in Andhra Pradesh, Kerala, Maharashtra and Rajasthan are highest as compared to other states.
2) Higher Cyber crimes registered in these states also shows that cyber criminals of age group 18-30 years are higher in number.
3) Maharashtra is again ahead in arresting cyber criminals of age group 18-30 years.
4) Age group 18-30 years indicates students, employees from education, Technology fields Education in these states is advance as well as these states are rich in natural resources, growing economically and technologically.

Table 9: Persons arrested under IT Act in States By Age Group Between 18-30 years (2009-13)

Sr.No.	States / Year	2009	2010	2011	2012	2013	Total
1	Maharashtra	50	88	140	215	214	**707**
2	Uttar Pradesh	15	40	52	60	213	**380**
3	Karnataka	9	56	30	35	45	**175**
4	Rajasthan	20	21	71	55	80	**247**
5	Andhra Pradesh	6	25	142	125	180	**478**
6	Kerala	25	61	86	81	73	**326**
7	Madhya Pradesh	20	27	63	105	104	**319**
8	Punjab	12	15	25	22	57	**131**
9	Gujarat	9	24	17	41	28	**119**
10	Tamil Nadu	5	28	18	20	18	**89**
11	Goa	0	1	4	3	4	**12**
	Total	**171**	**386**	**648**	**762**	**1016**	

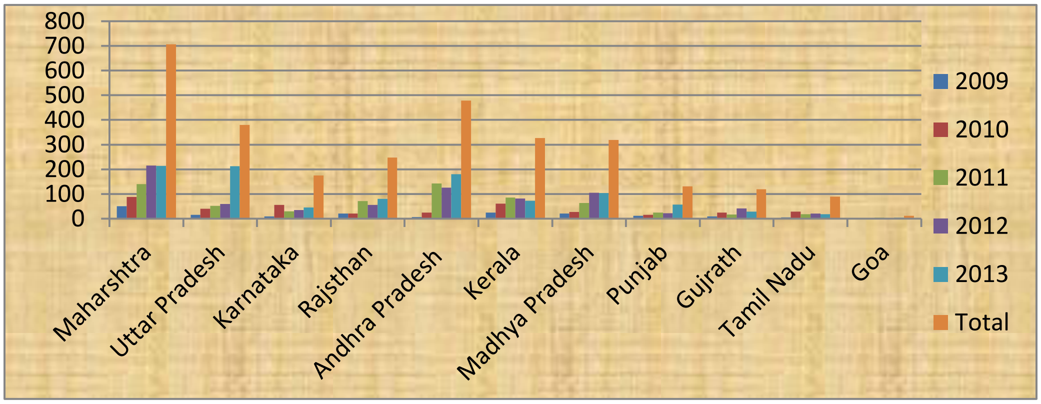


Figure 8: Persons arrested under IT Act in States between 18-30 years (2009-13)

`

INFERENCE: Figure 8 highlights the following facts on cyber crimes:

1) Persons arrested in Maharashtra, Andhra Pradesh, Kerala and Rajasthan are highest as compared to other states.
2) Higher Cyber crimes registered in these states also shows that cyber criminals of age group 18-30 years are also great in number.
3) Maharashtra is again ahead in arresting cyber criminals of age group 18-30 years.
4) Age group 18-30 years represents students, employees from education & Technology fields. Education in these states is advance as well as these states are rich in natural resources, growing economically and economically.

Table 10: Persons arrested under IT Act in States between 30-45 yrs (2009-2013)

States	**2009**	**2010**	**2011**	**2012**	**2013**	**Total**
Maharashtra	21	43	62	75	161	**362**
Uttar Pradesh	9	15	56	47	65	**192**
Karnataka	10	30	2	24	45	**111**
Rajasthan	0	14	26	18	42	**100**
Andhra Pradesh	2	46	83	35	94	**260**
Kerala	16	40	37	44	52	**189**
Madhya Pradesh	4	20	22	32	44	**122**
Punjab	4	17	12	56	58	**147**
Gujarat	1	19	13	23	14	**70**
Tamil Nadu	4	10	22	8	12	**56**
Goa	3	1	0	5	4	**13**
Total	**74**	**255**	**335**	**367**	**591**	

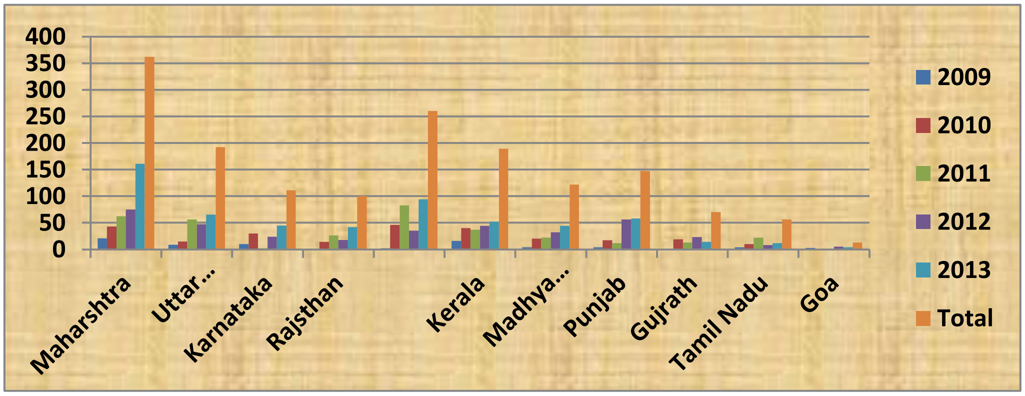


Figure 9: Persons arrested under IT Act between 30-45 years during (2009-2013)

`

INFERENCE: Figure 9 highlights the following facts on cyber crimes

1) Maharashtra shows highest number of cyber criminals arrested in the age group 30-45 years.
2) Andhra Pradesh, Uttar Pradesh, Kerala and Madhya Pradesh states are after Maharashtra in arresting persons between age group of 30-45 years.
3) These states have less number of cyber criminals of age group 30-45 years as compared to age group of 18-30 years.

Table 11: Incidences of Total cases registered and persons arrested under Cyber crimes (IT Act) during 2009-13 (All India)

Sr. No.	Crime Head	Cases registered during 2009-2013	Persons arrested during 2009-2013
1	Tampering source code Document	417	314
2	Hacking	6117	2713
3	Obscene Publication in electronic form	2755	2916
4	Unauthorized access to protected computers	45	55
5	Breach of Confidentiality/Privacy)	190	11

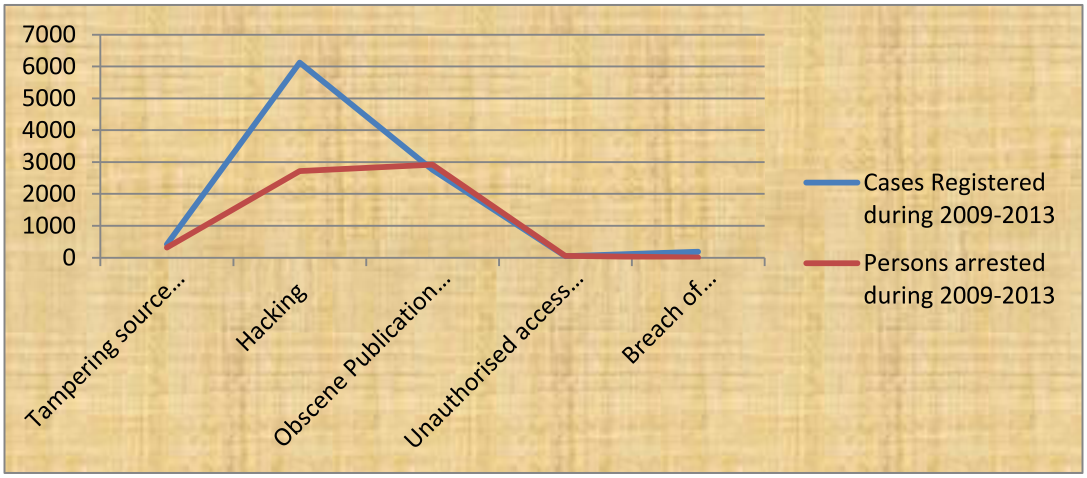


Figure 10 : Cases Registered Vs Persons arrested (2009-2013) [All India]

`

INFERENCE: Figure 10 highlights the following facts on cyber crimes:

1) The above table shows highest number of Hacking cases registered during 2009-13 in India.
2) The volume of crimes under 'Obscene publication in electronic form' is second lowest which is also a serious threat to the country.
3) Persons arrested during 2009-13 are very less for cyber crimes like tampering of source code, hacking and 'Obscene publication in electronic form' as compared to other crimes.

Table 12: Disposal of Cyber Crime Cases (IT Act) by Police during 2014-2015 [Maharashtra]

Crime Head	Cases for Investigation	Cases withdrawn or Investigated	Pending Cases
Tampering computer source Code (Section 65)	278	3	275
Computer related Offences (66 A-E)	18554	219	18335
Obscene Publication/ Transmission (67 A-C)	2368	22	2346

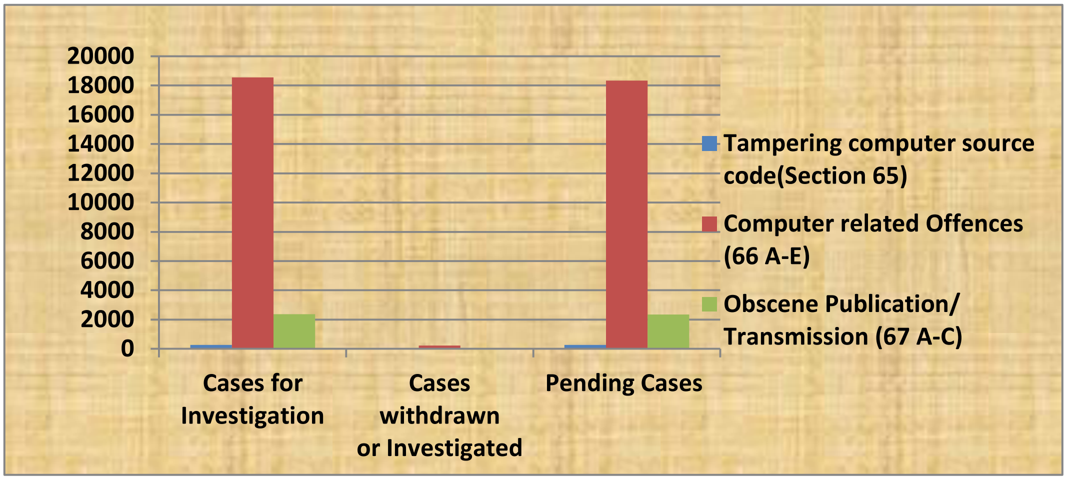


Figure 11: Disposal of Cyber Crime Cases (IT Act) by Police during 2014-15

INFERENCE: Figure 11 highlights the following facts on cyber crimes:

1) Cases registered under Section 66 (A-E) are highest as compared section 65 and Section 67. Cases under 66 (A-E) includes Computer related offences such as alteration with Computer source code, sending Offensive messages, Identity Theft, Hacking' etc. This is a threat to any individual, organization or nation.
2) The rate of cyber crime investigation is very poor i.e. 1.15 % which resulted in high number of pending cases.

4.3 – Best Practices of other countries for cyber security

The International telecommunication Union has released the Global Cyber Security Index for 2017. As per the findings of the Global Cyber Security Index for 2017, India ranks 23 out of the 193 member countries when it comes to commitment to cyber security. GCI Is a composite index that measures and compares the level of cyber security commitment amongst member states based on five pillars – technical, organizational, legal, cooperation and growth potential. The main objective of the Global Cyber Security Index is to measure the type, level and evolution of cyber security in countries from a global as well as regional perspective.

Singapore tops the charts with the highest level of cyber security commitment in the world and in the Asia Pacific region. As per the report, Singapore has a long history of cyber security practices from 2005. They made their first master plan for cyber security. The US comes in at the number 2, Malaysia number 3, Oman 4, Estonia 5, Mauritius 6, Australia 7, Georgia 8, France 9, Canada 10. These are the top 10 countries in the list of total 193 nations.

Table 13: Top 10 Countries according to highest GCI index (2017)

Sr.No.	Countries
1	Singapore
2	USA
3	Malaysia
4	Oman
5	Estonia
6	Mauritius
7	Australia
8	Georgia
9	France
10	Canada

As far as India is concerned GCI categorizes India in "Maturing stage" which refers to countries with a GCI score between 50 and 89 percentile. Countries are categorized as such because they have developed complex commitments and engage in cyber security programmes and initiatives. India does well in terms of legal cyber security measures but falls short on

- Technical measures
- Cooperation due to lack of standardization
- public-private partnership etc.

GCI Groups

Member States were classified into three categories by their GCI score.

Initiating stage refers to the 96 countries (i.e., GCI score less than the 50thpercentile) that have started to make commitments in cyber security.

Maturing stage refers to the 77 countries (i.e., GCI score between the 50th and 89th percentile) that have developed complex commitments, and engage in cyber security programmes and initiatives.

Leading stage refers to the 21 countries (i.e., GCI score in the 90th percentile) that demonstrate high commitment in all five pillars of the index.

Cyber security is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective.
It is important to develop a Cyber security culture where citizens are aware of the risks and monitoring when using electronic networks.

Table 14: The Top 14 Cyber Aware Countries as per GCI index

Sr. No.	Country	Rank	GCI Awareness Score
1	USA	1	0.824
2	Canada	2	0.794
3	Australia	3	0.765
4	Malaysia		
5	Oman		
6	New Zealand	4	0.735
7	Norway		
8	Brazil	5	0.706
9	Estonia		
10	Germany		
11	India		
12	Japan		
13	South Korea		
14	UK		

`

Best Practices/Effective Policies of Top 5 countries in the world on Cyber Security:

According to GCI index, Best practices of Top 5 Countries were studied which highlighted following important aspects.

1) **USA:**

   Industrial Control System Cyber Emergency Response Team (ICS-CERT) provides focused operational capabilities for defense of control system environment against emerging cyber threats.

   The public sector professionals and national agencies are provided cyber security framework for the certification and accreditation.

   US has International Strategy for Cyber space from 1996.

   IT security practitioners are required to pass a national baseline of essential knowledge and skills set by IT Security Essential Body of knowledge (EBK) in order to perform specific roles and responsibilities.

2) **Canada:**

   Canada has following Institutes for promoting cyber security of their country.

   a) Anti Spam Law
   b) Canadian Anti fraud center
   c) Defense Research and Development Canada
   d) Canadian Cyber Indian Response Center
   e) Communications Security Establishment Canada (CSEC)
   f) Information Technology Incident Management Plan
   g) Cyber Security Self-Assessment Guidance for Federally regulated Financial Institutions

3) **Australia:**

   Australia Government has agency that provides guidance about cyber scams and how to report them.

`

The Australian Federal Police (AFP)has technical wing under them which is responsible for investigating high technical issues. It also has separate arm that investigates scams relating to financial services such as phishing.

4) **New Zealand:**

New Zealand provides enhanced services in defending against cyber borne threats to Government. Cyber security standards, best practices and guidelines are provided by New Zealand's Unitec, its first cyber security center.

5) **Germany:**

Germany has a cyber Security Strategy and National Plan for information Infrastructure Protection (NPSI). They have national and sector specific Cyber security strategy.

Complaints related to child abuse and other online illegal content can be filed online.

4.4 - The Cyber Crime Scenario In Maharashtra (2009-2011) [through RTI]

Study of cyber crime reports obtained from various cyber cells of Maharashtra through RTI (Right To Information Act) for the period 2009-2011

`

4.4.1 Organisational Structure of Cyber Crime Investigation

Following is the general Organisational Structure of Cyber Crime Investigation of Maharashtra.

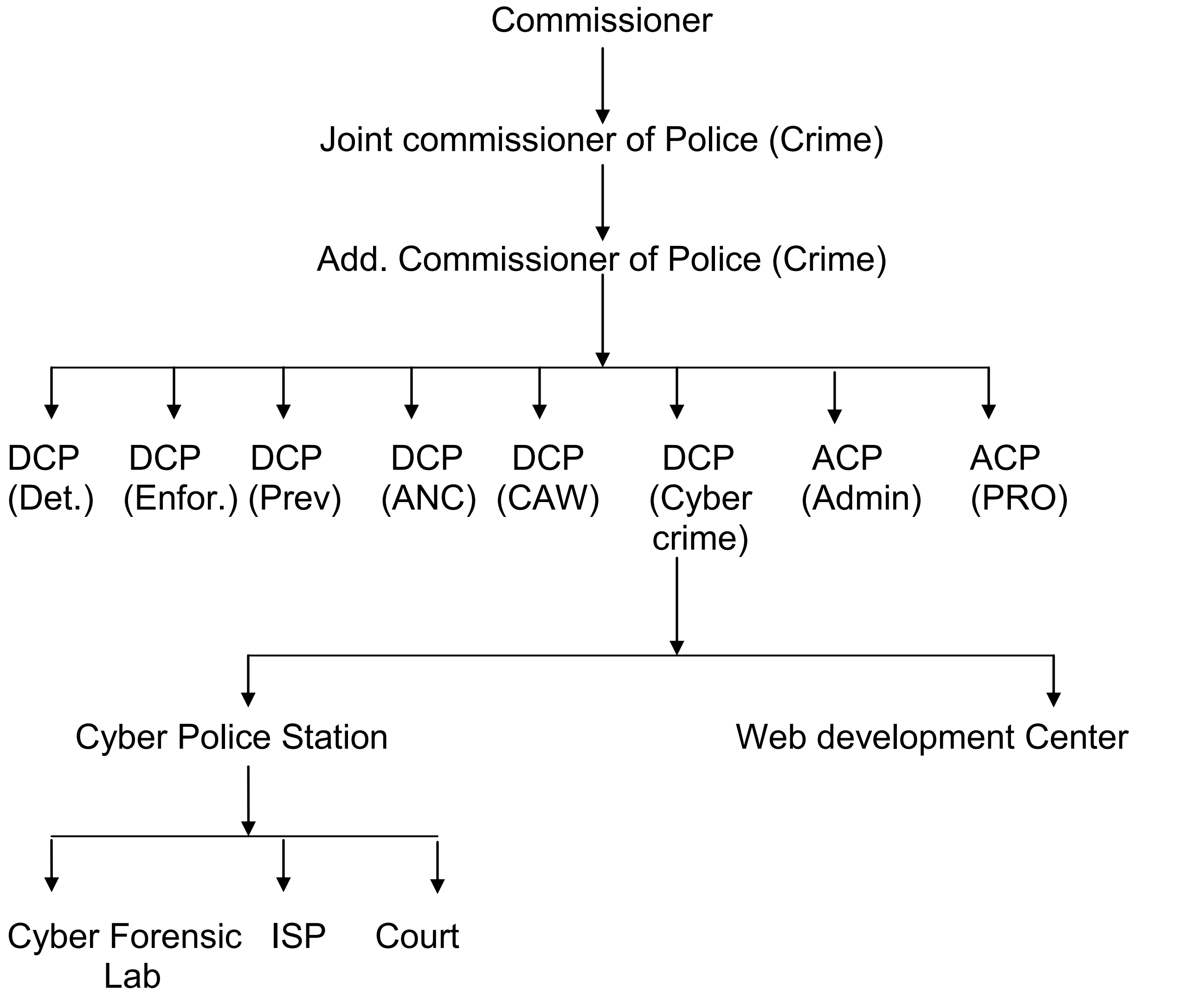


Figure 12: Organizational Structure of Cyber Crime Investigation

Joint Commissioner of Police (Crime) comes under Commissioner of Police, is responsible for Crime Prevention, Detection and Investigation.

DCP (Cyber Crime) is Overall in-charge of Cyber Police Station and Web Development Centre.

Cyber Police Station: This branch deals with the investigation of website hacking, cyber stalking, cyber pornography, e-mail, credit card crime, software piracy, on-line fraud and internet crime.

`

4.4.2 Study of report given by Cyber Forensic Science Laboratories, Santa Cruz (Mumbai), Maharashtra state (Dt. 7.11.12)

Following information on Cyber crimes during 2009-11 was received from Directorate of Forensic Science Laboratories, Home Department, Santa Cruz, Mumbai, Maharashtra state on 7.11.12.

Table 15: Cyber crime Statistics from 2009-Jan 2012 given by Cyber Forensic Lab -Santa Cruz, Mumbai (Dt. 7.11.12)

Types of Cyber crimes	**Year**	**Cases Registered**	**Number of Crimes Resolved**	**Cyber crimes under Investigation**	**Pending cases with reasons**
E-mail theft, Data Theft, Web Site Hacking, Phishing, Credit Card Frauds	2009	171	94	305	At, 31 Jan 2012, 571 cases were pending. Reason is **inadequate staff** and subsequently **huge receipt of cases from all over Maharashtra.**
	2010	270	156	413	
	2011	345	206	556	
	Jan-2012	31	16	571	

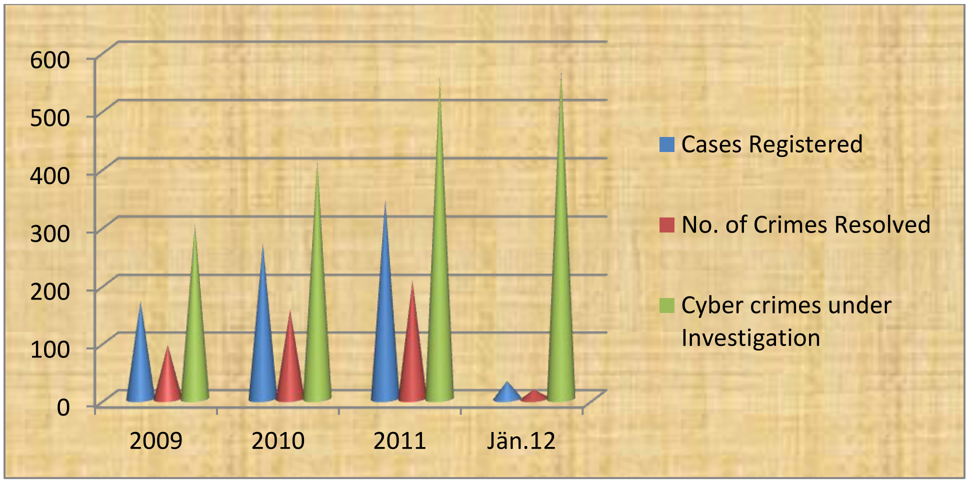


Figure 13: Cyber crimes status from 2009 to Jan-2012

`

INFERENCE:

1) Above graph shows rise in cyber crimes from 2009 to Jan-2012along with huge number of '**cases pending/under investigation'** in Maharashtra.
2) Authorities are highlighting 2 main reasons of pending cases as follows.
   - **Inadequate staff for Cyber Crime investigation**
   - **Huge Receipt of cases from all over Maharashtra**
3) Cyber Crime Status from 2009-11 shows that cyber crimes are increasing greatly in Maharashtra.

Therefore, the above two reasons given by Government authorities strengthens the Research problem selected for Ph.D. study i.e. "Factors affecting effective investigation of cyber crimes".

`

4.4.3 Study of Cyber Crime Report Given By Cyber Cell, Crime Branch, Thane, Maharashtra State (Dt. 22.11.12)

Report of Cyber crimes received from Cyber cell, Crime branch, Thane (Dt. 22/11/2012) given by Government Information Officer and Asst. Police Commissioner, Crime branch, Thane as follows.

Table 16: Cyber crimes during 2009-11 in Thane (Mumbai)

Total Cyber Crimes in Thane	**66**
Data theft	4
Phishing	35
Credit Card Frauds	27
Email Threats	Nil
Web site hacking	Nil

INFERENCE:

1) As per the furnished information in Table 16, Email Threats and Website hacking information was Nil. No Record of these cyber crimes from 2009-11.
2) The number of Cyber crimes registered for Data Theft, Phishing, and Credit Card Frauds were 4, 35, 27 respectively. Crimes on Phishing and Credit card frauds were significant.

Table 17: Cyber Crimes as per IT ACT (under sections 65, 66, 67)

IT ACT (2000)	**Crimes under Section**
Section 65	1
Section 66 A , B	5
Section 66 C	46
Section 66 D	39
Section 67	1

INFERENCE: Table 17 shows that cyber crimes registered under IT Act (2000) under Section 66 A,B ; Section 66 C and Section 66 D are more as compared to Section 65 and Section 67.

Table 18: Cyber Crimes Investigation Status (Total: 66)

During 2009-11 in Thane

Cyber Crime Case Status	**No.**
Final	24
Compoundable + Disposed	1
Under Investigation	8
Court Pending	8

INFERENCE:

1) Table 14 shows that out of 66 cases, 24 cases are final, 1 is Compoundable + Disposed, 8 are under investigation and 8 are court pending. This shows that approximately 62% cases are pending in 3 years after registration which is a serious threat.

`

4.4.4 Study Of Report Given By Cyber Cell, Crime Branch, Mumbai Dt. 26/11/2012

Report of Cyber crimes received from Cyber cell, Crime branch, Mumbai (Dt.26/11/2012) given by Government Information Officer and Asst. Police Commissioner, Crime branch, Mumbai as follows.

Table 19: Information of Cyber Crime cases (year 2009-11)
(Source: Cyber Cell, Crime branch, Mumbai Dt. 26/11/2012)

Type of Cyber crime	**No. of Crimes Reported /Registered**				**No. of Cyber Crimes Resolved**				**No. of Crimes under Investigation**				**Pending cases with reason**			
	2009	**2010**	**2011**	**2012**	**2009**	**2010**	**2011**	**2012**	**2009**	**2010**	**2011**	**2012**	**2009**	**2010**	**2011**	**2012**
Email Threat	4	1	2	-	4	-	2	-	0	1	0	0	-	Under investi -gation	-	-
Data Theft	2	-	1	1	2	-	1	-	0	-	0	1	-	-	-	Under Investigation
Website Hacking	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Phishing	-	-	-	1	-	-	-	-	-	-	-	1	-	-	-	Under Investigation
Credit Card Fraud	-	-	-	2	-	-	-	1	-	-	-	1	-	-	-	Under Investigation

INFERENCE:

1) From above Table 15, it can be seen that cyber crimesrelated to Email-Threat and Data Theft are significant in these 3 years in Mumbai region. Pending cases are under investigations.

`

Table 20: Summary Table (based on Table 19) showing Cyber crimes status from 2009-11 in Mumbai.

Type ofCyber crime	Total Cyber Crimes	Cyber crimes Under Investigation
Email Theft	7	1
Data Theft	4	1
Website Hacking	0	0
Phishing	1	1
Credit card Fraud	2	1

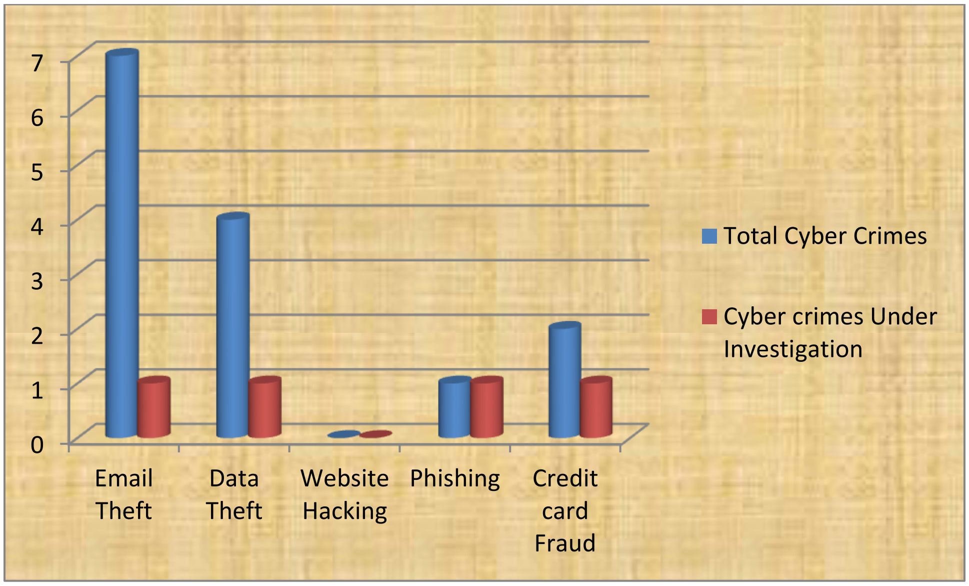


Figure 14: Cyber Crime status 2009-2011 in Mumbai (Cases Registered Vs under Investigation)

INFERENCE:

This information shows that, out of 14 cyber crimes reported in Mumbai during 2009-11, 4 cases are under investigation which is 28%.

4.4.5 Study Of Report Given By Cyber Cell, Crime branch, Pune Dt. 5/12/2012

Report of Cyber crimes received from Police Department and Public Information officer, Cyber cell, Crime branch, Pune (Dt. 5/12/2012)is as follows.

Table 21: Information of Cyber Crime cases (year 2009-2012) in Pune

Type of Cyber crime	**No. of Cyber Crimes Reported /Registered**				**No. of Cyber Crimes Resolved**				**No. of Cyber Crimes Pending**				**Pending cases with reason**			
	2009	**2010**	**2011**	**2012**	**2009**	**2010**	**2011**	**2012**	**2009**	**2010**	**2011**	**2012**	**2009**	**2010**	**2011**	**2012**
Email Threat	-	2	8	5	-	1	6	4	-	-	-	1	-	-	-	All cases are under investigation
Data Theft	-	3	2	4	-	1	2	3	-	-	-	1	-	-	-	
Website Hacking	-	1	5	4	-	-	4	3	-	-	-	1	-	-	-	
Phishing	4	52	56	22	2	28	38	18	-	-	8	8	-	-	-	
Credit card Fraud	3	15	22	30	1	4	13	20	-	-	5	6	-	-	Under Investigation	

Summary of Cyber Crime report of Pune city based on information given by Cyber cell, Pune (Dt. 5/12/12) from the year 2009-2012 is as follows.

`

Table 22: Summary of Cyber crimes status of Cases registered Vs Cases Pending during 2009-12 in Pune city

Type of Cyber crime	Number of Crimes Reported /Registered	Number of Cyber Crimes Resolved	Number of Cyber Crimes Pending	Status
Email Threat	15	11	4	All cases are under investigation.
Data Theft	9	6	3	
Website hacking	10	7	3	
Phishing	134	86	84	
Credit card fraud	70	38	32	

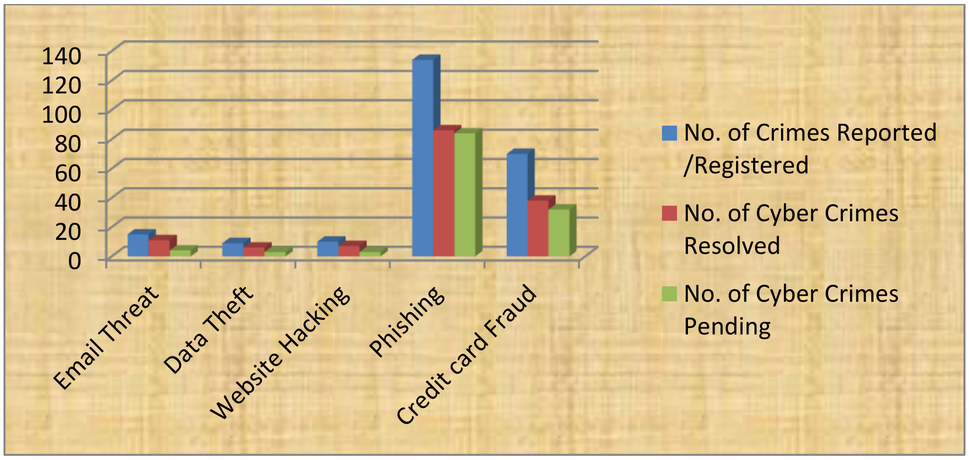


Figure 15: Cases registered Vs Cases Pending during 2009-12 in Pune city

INFERENCE:

1) This report shows that in Pune, the highest number of Phishing cases registered were 134 in the last 4 years (2009-2012) whereas Cases Resolved were only 86 and pending cases were 84 i.e. approx. 62 % cases of Phishing are pending.
2) Credit card Theft cases registered are 70 in last 4 years whereas Cases Pending are 32 i.e. approx. 46 % cases of Credit card Theft are pending.

All these statistics shows that there is need of faster investigation of cyber crimes, otherwise it creates room for cyber criminals to commit more cyber crimes.

`

Chapter 4.5 Analysis of Cyber crime scenario in Pune City [through RTI]

The information of cyber crimes in Pune region is obtained from all 39 police stations in Pune city and PCMC area. This information was obtained via RTI which gives the authenticity and reliability of given information from all police stations. This data covers cyber crimes under IT Act under U/s 65, 66 (A-E), 67. The reason to select theses section is that from literature review it is observed that most of the cyber crimes occurred under these sections.

Initially all police stations were communicated via personal visit and questionnaire sent to them using RTI via registered id.

The analysis of the collected data on cyber crimes in Pune region was carried out step by step as follows :

1) List of Respondents on cyber crimes from Pune City
2) Police stations wise Cyber Crimes Registered, Resolved, Pending in Pune City during 2011-2016
3) Yearwise Cyber Crimes Registered, Resolved and Pending in Pune City during 2011-2016
4) Pending Cyber Crime status (2011-2016) in Pune
5) Status of Cyber Crimes U/s 65 in Pune City (Year 2011-2016)
6) Status of Cyber Crimes U/s 66 (A-E) in Pune City (Year 2011-2016)
7) Status of Cyber Crimes U/s 67 in Pune City (Year 2011-2016)

`

Table 23: List of Respondents on cyber crimes from Pune City

SNo.	Division	No.	Name of Police Station	Information Received Yes/No
1	**Chaturshringi Division**	1	Wakad Police Station	YES
		2	Sangavi Police Station	YES
		3	Hinjewadi Police Station	YES
		4	Chaturshringi Police Station	NO
2	**Pimpri Division**	5	Pimpri Police Station	YES
		6	Chinchwad Police Station	YES
		7	Nigadi Police Station	YES
		8	Bhosari Police Station	YES
		9	MIDC Bhosari Police Station	YES
3	**Khadaki Division**	10	Yerawada Police Station	YES
		11	Vimantal Police Station	YES
		12	Vishrantwadi Police Station	YES
		13	Khadaki Police Station	YES
		14	Dighi Police Station	YES
		15	Chandan Nagar Police Station	YES
4	**Wanavdi Division**	16	Mundhawa Police Station	YES
		17	Hadapsar Police Station	YES
		18	Kondhwa Police Station	YES
		19	Wanawadi Police Station	YES
5	**City Division**	20	Faraskhana Police Station	YES
		21	Khadak Police Station	NO
6	**Vishrambaug Division**	22	Vishrambaug Police Station	YES
		23	Shivajinagar Police Station	YES
7	**Deccan Division**	24	Deccan Police Station	YES
		25	Kothrud Police Station	YES
		26	WarjeMalwadi Police Station	NO
8	**Swargate Division**	27	BharatiVidyapeeth Police Station	NO
		28	Sahakar Nagar Police Station	YES
		29	Market Yard Police Station	YES
		30	Sinhagad Police Station	NO
		31	Bibvewadi Police Station	YES
		32	Dattawadi Police Station	NO
		33	Swargate Police Station	YES
9	**Lashkar Division**	34	Bund Garden Police Station	YES
		35	Koregaon Park Police Station	YES
		36	Lashkar Police Station	YES
		37	Samarth (Somwarpeth) Police Station	YES
10	**Commissioner Office**	38	Cyber Crime Cell, Crime Branch, Pune	YES
		39	Pune Crime Branch, Pune	YES

`

INFERENCE:

1) From Pune City, out of 39 police stations out of 6 Divisions, personnel in 34 Police stations responded to the Questionnaires on cyber crimes.

2) 6 Police station personnel had not submitted the data. The Percentage of respondents is 84.61% i.e. approximately 85% which makes the research work more authentic. The research data has been obtained under Right to Information Act (RTI Act). Therefore it can be considered more reliable.

Table 24:Police stations wise Cyber Crimes Registered, Resolved, Pending in Pune City during 2011-2016

(Note: Yellow mark highlights that there is no data given by these police stations)

Year	2011			2012			2013			2014			2015			2016			Police station wise Total Cyber crimes (2011-16)		
Police stations	Registered	Resolved	Pending	Registered	Resolved	Pending	Registered	Resolved	Pending	Registered	Resolved	Pending	Registered	Resolved	Pending	Registered	Resolved	Pending	Registered	Resolved	Pending
1. Sangavi	0	0	0	2	2	0	4	4	0	4	1	3	9	2	8	11	6	9	**30**	**15**	**20**
2.Yerwada	17	0	20	13	0	13	4	0	4	54	11	43	44	1	43	37	22	15	**169**	**34**	**138**
3.Vimantal	2	2		7	4	7	3	3	3	6	3	3	2	0	3	0	0	0	**20**	**12**	**16**
4.Vishrant wadi	1	1	0	2	2	0	2	2	0	8	8	0	8	6	2	3	0	3	**24**	**19**	**5**
5.Khadki	2	0	2	1	0	1	1	0	1	0	0	0	3	0	3	3	0	3	**10**	**0**	**10**
6. Dighi	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	**1**	**0**	**1**
7.Chandan Nagar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8.Mundwa	1	0	1	1	0	1	1	0	1	1	0	1	6	0	6	4	0	4	**14**	**0**	**14**
9.Wanwadi	3	3	0	4	2	2	2	2	0	7	3	4	6	4	2	8	0	8	**30**	**14**	**16**
10. Hadapsar	5	1	4		3	1	2	0	2	5	1	4	6	1	5	15	0	15	**33**	**6**	**31**
11. Kondhwa	2	2	0	6	6	0	5	3	2	8	1	7	11	6	5	5	1	4	**37**	**19**	**18**
12. Faraskhana	2	2	0	2	2	0	0	0	0	2	2	0	4	4	0	4	3	1	**14**	**13**	**1**
13. Khadak	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14. Shivajinagar	2	2	0	2	2	0	2	2	0	5	5	0	4	2	2	3	0	3	**18**	**13**	**5**
15. Vishrambag	7	7	0	2	2	0	6	6	0	3	3	0	1	1	0	3	3	0	**22**	**22**	**0**
16. Deccan	31	23	8	3	1	2	10	4	6	23	5	18	49	10	39	3	0	3	**119**	**43**	**76**
17. Kothrud	0	0	0	0	0	0	7	2	5	16	3	13	6	3	3	14	5	9	**43**	**13**	**30**
18. Sahkarnagar	0	0	0	0	0	0	3	2	1	4	1	3	8	0	8	0	0	0	**15**	**3**	**12**
19. Marketyard	0	0	0	0	0	0	1	0	1	1	0	1	1	0	1	1	0	1	**4**	**0**	**4**
20. Bibvewadi	0	0	0	0	0	0	0	0	0	8	0	8	0	0	0	1	0	1	**9**	**0**	**9**
21. Dattawadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22. Swargate	1	1	0	0	0	0	3	3	0	2	2	0	2	1	1	4	0	4	**12**	**7**	**5**
23.Bund Garden	0	0	0	0	0	0	0	0	0	0	0	0	27	3	24	21	3	18	**48**	**6**	**42**
24. Samarth	0	0	0	1	0	1	2	0	2	2	0	2	6	3	3				**11**	**3**	**8**
25.Koregaon Park	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26.Lashkar	20	18	2	14	14	0	2	2	0	47	37	10	25	4	21	14	3	11	**122**	**78**	**44**
27. Wakad(2014)	0	0	0	0	0	0	0	0	0	1	1	0	2	1	1	12	0	12	**15**	**2**	**13**
28. Hinjewadi	0	0	0	0	0	0	0	0	0	5	0	0	9	0	0	12	8	4	**26**	**8**	**4**
29. Pimpri	4	0	4	6	3	3	0	0	0	5	0	5	6	0	6	9	1	8	**30**	**4**	**26**
30. Chinchwad	4	4	0	10	10	0	4	4	0	8	8	0	2	0	2	6	2	4	**34**	**28**	**6**
31. Nigadi	4	0	4	2	0	2	2	0	2	6	0	6	3	0	3	8	0		**25**	**0**	**17**
32. Bhosari	1	0	1	0	0	0	1	0	1	6	1	5	3	0	3	5	3	2	**16**	**4**	**12**
33. MIDCBhosari	0	0	0	0	0	0	2	2	0	6	6	0	0	0	0	1	0	1	**9**	**8**	**1**
34. Sangavi	0	0	0	2	2	0	4	4	0	4	1	3	9	4	5	11	6	9	**30**	**17**	**17**
35.Cyber Cell	0	0	0	0	0	0	63	33	29	158	54	104	161	70	89	0	0	0	**382**	**157**	**222**
Total	**109**	**66**	**46**	**80**	**55**	**33**	**136**	**78**	**60**	**405**	**157**	**243**	**424**	**126**	**289**	**218**	**66**	**152**	**1004**	**548**	**823**

`

Table 25: Yearwise Cyber Crimes Registered, Resolved and Pending in Pune City during 2011-2015

Cyber crimes /Year	2011	2012	2013	2014	2015
Registered	109	80	136	405	424
Resolved	66	55	78	157	126
Pending	46	33	60	243	289

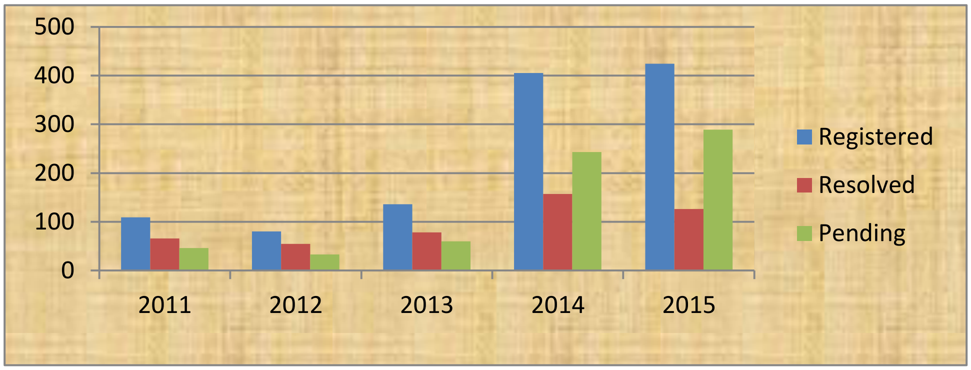


Figure 16: Yearwise Cyber Crimes Registered, Resolved and Pending in Pune City during 2011-2015

INFERENCE:

1) From the above figure it is observed that Crimes Registered during 2011-15are increasing drastically.
2) The Rate of Cyber crimes Resolved is very less and gradually decreasing from 2011 which is a matter of serious concern. (e.g., 2011-60.55%, 2012-68.75 %, 2013-57.35%, 2014-38.76% and 2015 it is 29.71 %).
3) Therefore rate of Pending cyber crimes seen in theses last 5 years is also increases which is a boon for cyber criminals

`

Table 26: Pending Cyber Crime status (2011-2016) in Pune

	Police stations	Police station wise			
		Total Cyber crimes (2011-16)			
SNo.		Registered	Resolved	Pending	% of Pending crimes
1	Sangavi	30	15	20	66.67
2	Yerawada	169	34	138	81.66
3	Vimantal	20	12	16	80.00
4	Vishrantwadi	24	19	5	20.83
5	Khadki	10	0	10	100.00
6	Dighi	1	0	1	100.00
7	ChandanNagar	0	0	0	0.00
8	Mundhwa	14	0	14	100.00
9	Wanwadi	30	14	16	53.33
10	Hadapsar	33	6	31	93.94
11	Kondhwa	37	19	18	48.65
12	Faraskhana	14	13	1	7.14
13	Khadak	0	0	0	0.00
14	Shivajinagar	18	13	5	27.78
15	Vishrambag	22	22	0	0.00
16	Deccan	119	43	76	63.87
17	Kothrud	43	13	30	69.77
18	Sahkarnagar	15	3	12	80.00
19	Marketyard	4	0	4	100.00
20	Bibvewadi	9	0	9	100.00
21	Dattawadi	0	0	0	0.00
22	Swargate	12	7	5	41.67
23	BundGarden	48	6	42	87.50
24	Samarth	11	3	8	72.73
25	KoregaonPark	0	0	0	0.00
26	Lashkar	122	78	44	36.07
27	Wakad	15	2	13	86.67
28	Hinjewadi	26	8	4	15.38
29	Pimpari	30	4	26	86.67
30	Chinchwad	34	28	6	17.65
31	Nigadi	25	0	17	68.00
32	Bhosari	16	4	12	75.00
33	MIDC Bhosari	9	8	1	11.11
34	Sangavi	30	17	17	56.67
35	Cyber Cell	382	157	222	58.12

`

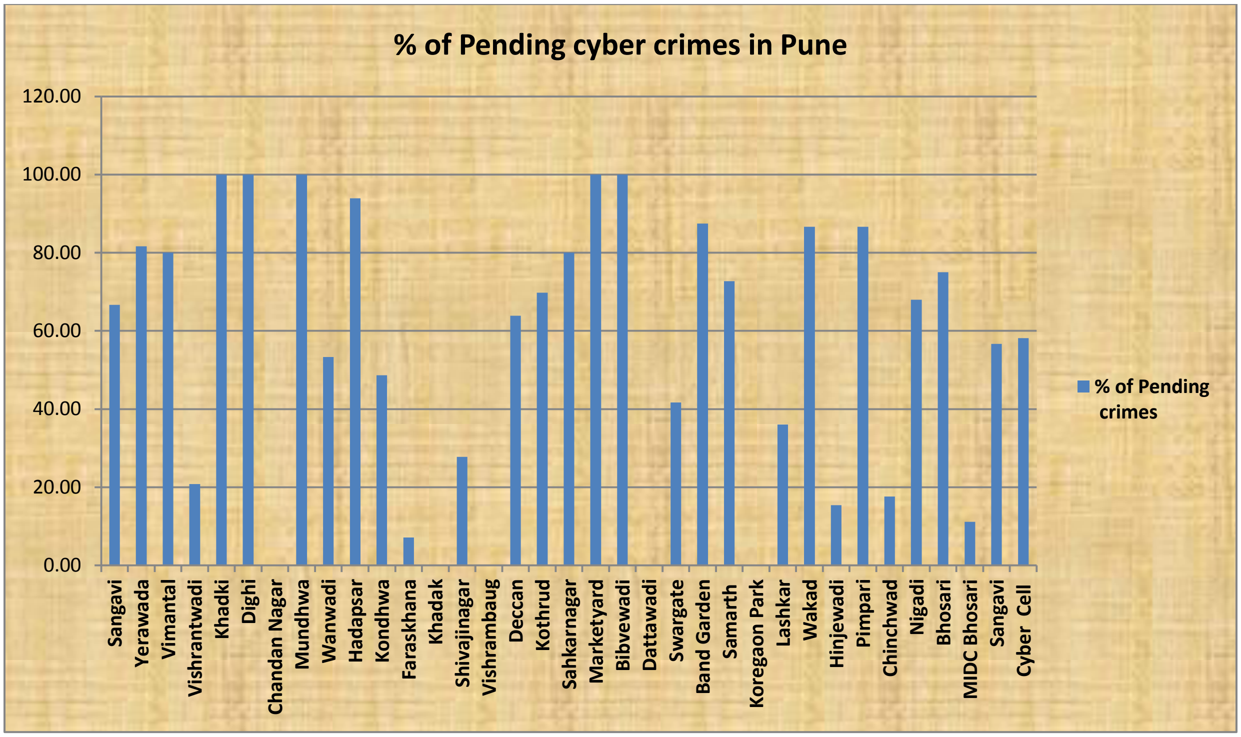


Figure 17: Percentage (%) of Pending cyber Crime in Pune

INFERENCE:

1) Table 26 shows that in Pune city, police stations having maximum number of registered cyber crimes in last five years (2011-16) are Yerawada, Deccan, Bund Garden, Lashkar and Cyber Cell where percentage of cases pending are 81.66% , 63.87%, 87.50%, 36.07% and 58.12% respectively. This must be given proper attention by these police stations.
2) Police stations Khadaki, Dighi, Mundhwa, Market yard and Bibwewadi have very less number of cyber crimes but the Percentage of pending crimes is **100%** which is a matter of serious concern.
3) Figure 17 above shows that almost all police stations have more than 50% pending crimes.

`

Table 27: Status of Cyber Crimes u/s 65 in Pune City (Year 2011-2016)
(Note: Yellow mark highlights that there is no data given by these police stations)

	Section 65																	
Police stations	Crimes Registered						Crimes Resolved						Crimes Pending					
	2011	2012	2013	2014	2015	2016	2011	2012	2013	2014	2015	2016	2011	2012	2013	2014	2015	2016
Yerawada	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Vimantal	0	0	0	0	0	_	0	0	0	0	0	_	0	0	0	0	0	_
Vishrantwadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Khadki	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Dighi	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Chandannagar	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Mundhwa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wanwadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hadapsar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Kondhwa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Faraskhana	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Khadak	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Shivajinagar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Vishrambaug	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Deccan	0	0	0	2	3	2	0	0	0	1	1	0	0	0	0	1	2	2
Kothrud	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sahkarnagar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Marketyard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bibwewadi	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1
Dattawadi	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Swargate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bund Garden	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Samarthnagar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KoregaonPark	0	0	0	0	0	6	0	0	0	0	0	4	0	0	0	0	0	2
Lashkar	2	0	1	9	2	1	2	0	1	8	0	0	0	0	0	1	2	1
Wakad	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hinjewadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Pimpari	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Chinchwad	4	5	2	4	1	3	4	5	2	4	1	1	0	0	0	0	0	2
Nigadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bhosari	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-
MIDC Bhosari	NA	0	0	0	0	0	NA	0	0	0	0	0	NA	0	0	0	0	0
Sangavi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cyber Cell	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cybercrime status in Pune	**7**	**5**	**3**	**16**	**6**	**13**	**6**	**5**	**3**	**13**	**2**	**5**	**1**	**0**	**0**	**3**	**4**	**8**

`

Table 28: Yearwise Cyber Crimes under Section 65 Registered, Resolved and Pending in Pune City during 2011-2016

	2011	2012	2013	2014	2015	2016
Registered	7	5	5	16	6	13
Resolved	6	5	3	13	2	5
Pending	1	0	0	3	4	8

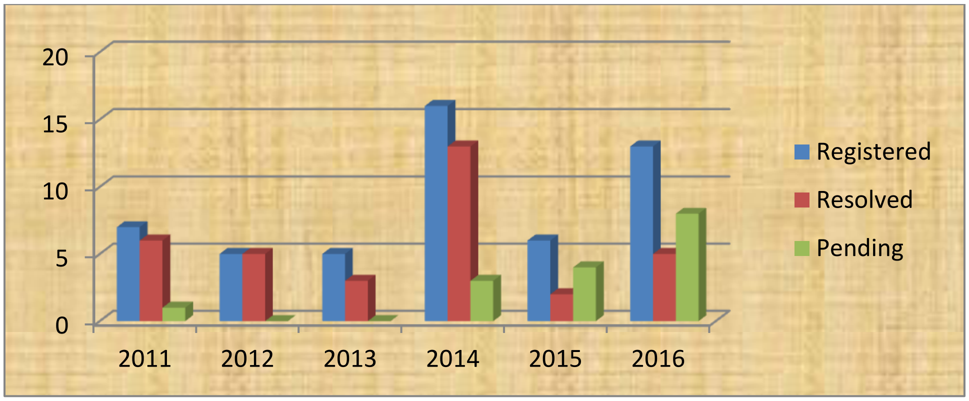


Figure 18: Yearwise Cyber Crimes under Section 65 Registered, Resolved and Pending in Pune City during 2011-2016

INFERENCE:

1) Cyber crimes coming under Section 65 (Phishing) are seen very negligible in all areas of Police stations in Pune city except Deccan, Lashkar and Chinchwad.
2) There is no significant rise in these types of crime.
3) Under section 65, Deccan, Lashkar and Chinchwad areas have more number of registered cyber crimes out of total cyber crimes than any other police stations.

Table 29: Cyber Crimes Registered, Resolved & Pending u/ Section 66 A to E

	2011	2012	2013	2014	2015	2016
Registered	38	38	46	157	145	139
Resolved	9	14	20	53	34	33
Pending	32	24	26	106	111	101

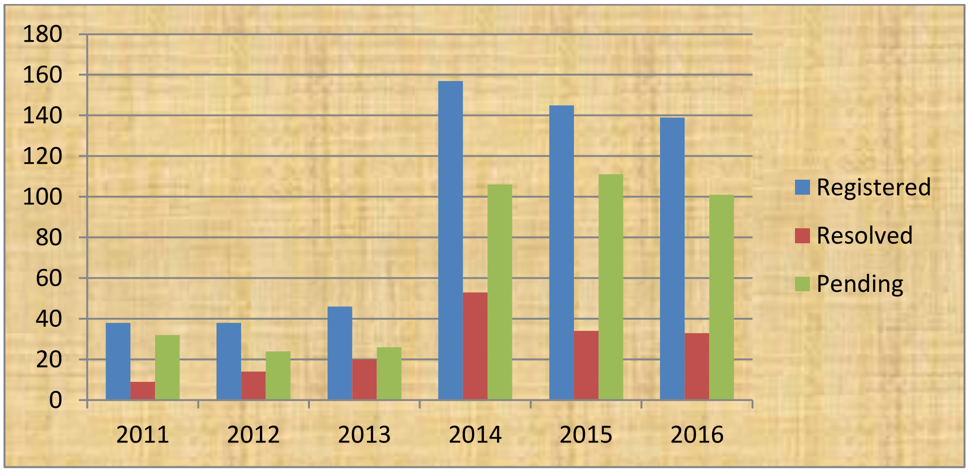


Figure 19:Yearwise Cyber Crimes under Section 66 Registered, Resolved and Pending in Pune City during 2011-2016

INFERENCE:

1) There is significant rise in cyber crimes under Section 66 of IT Act from 2011 to 2016.
2) In the last 5 years, the crimes increased 4 times as compared to 2011.
3) The Percentage of Crimes resolved is between 20-45% in last 5 years which is a matter of serious concern.
4) The Percentage of Crimes Pending is 72-85% in last 5 years which is a matter of serious concern.

`

(Note: Yellow mark highlights that there is no data given by theses police stations)

Table 30: Status of Cyber Crimes u/s 66 A to E in Pune City Year 2011-2016

	Section 66 A to E																	
Police stations	**Crimes Registered**						**Crimes Resolved**						**Crimes Pending**					
	2011	**2012**	**2013**	**2014**	**2015**	**2016**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
Yerawada	9	9	3	32	27	19	0	0	0	6	0	3	12	9	3	27	27	8
Vimantal	1	1	1	3	2	_	1	1	1	1	0	_	0	0	0	3	2	_
Vishrantwadi	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Khadki	2	1	1	0	1	2	0	0	0	0	0	0	2	1	1	0	1	2
Dighi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ChandanN.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mundhwa	1	1	1	1	6	3	0	0	0	0	0	0	1	1	1	1	6	3
Wanwadi	0	2	0	1	0	5	0	2	0	1	0	0	0	0	0	0	0	5
Hadapsar	5	3	2	4	6	15	1	1	0	1	0	0	4	2	2	3	6	15
Kondhwa	2	3	3	3		4	2	3	2	0	1	0	0	0	1	3	2	4
Faraskhana	2	2	0	1	4	4	2	2	0	1	4	4	0	0	0	0	0	0
Khadak	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Shivajinagar	2	2	2	4	4	2	0	0	0	0	2	0	2	2	2	4	2	2
Vishrambaug	5	2	0	3	0	0	1	1	0	3	0	0	4	1	0	0	0	0
Deccan	1	3	3	13	28	2	0	1	1	3	5	0	1	2	2	10	23	2
Kothrud	0	0	7	16	6	12	0	0	2	3	3	4	0	0	5	13	3	8
Sahkarnagar	0	0	2	2	4	0	0	0	2	1	0	0	0	0	0	1	4	0
Marketyard	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
Bibvewadi	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1
Dattawadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Swargate	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Bund garden	0	0	0	0	1	8	0	0	0	0	0	0	0	0	0	0	1	8
Samarth	0	1	2	2	6	0	0	0	0	0	0	0	0	1	2	2	6	0
KoregaonP.k	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0	0
Lashkar	2	0	0	9	2	1	2	0	0	8	0	0	0	0	0	1	2	1
Wakad	0	0	0	1	2	8	0	0	0	1	1	0	0	0	0	0	1	8
Hinjewadi	0	0	0	4	8	12	0	0	0	4	5	8	0	0	0	0	0	4
Pimpari	2	6	0	4	6	9	0	3	0	0	0	1	2	3	0	4	6	8
Chinchwad	0	0	2	4	1	1	0	0	2	4	0	0	0	0	0	0	1	1
Nigadi	4	2	2	6	3	8	0	0	0	0	0	0	4	2	2	6	3	8
Bhosari	0	0	0	5	3	5	0	0	0	0	0	0	0	0	0	5	3	5
MIDC Bhosari	NA	0	1	3	0	0	NA	0	1	3	0	0	NA	0	0	0	0	0
Sangavi	0	0	3	3	6	8	0	0	3	1	3	5	0	0	0	2	3	6
Cyber Cell	0	0	11	30	18	0	0	0	6	12	10	0	0	0	5	18	8	0
Total crimes	**38**	**38**	**46**	**157**	**145**	**139**	**9**	**14**	**20**	**53**	**34**	**33**	**32**	**24**	**26**	**106**	**111**	**101**

`

Table 31: Status of Cyber Crimes u/s 67 in Pune City Year 2011-2016

(Note: Yellow mark highlights that there is no data given by theses police stations)

	Section 67																	
	Crimes Registered						Crimes Resolved						Crimes Pending					
Police stations	2011	2012	2013	2014	2015	2016	2011	2012	2013	2014	2015	2016	2011	2012	2013	2014	2015	2016
Yerawada	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0
Vimantal	0	0	1	1	0	_	0	0	1	0	0	_	0	0	0	1	0	_
Vishrantwadi	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Khadki	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Dighi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ChandanNgar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mundhwa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wanwadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hadapsar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Kondhwa	0	3	0	0	0	1	0	3	0	0	0	1	0	0	0	0	0	0
Faraskhana	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Khadak	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Shivajinagar	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1
Vishrambaug	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Deccan	1	0	2	0	0	1	1	0	1	0	0	0	0	0	1	0	0	1
Kothrud	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
Sahkarnagar	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2	0
Marketyard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bibvewadi	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Dattawadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Swargate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bund Garden	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Samarth	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0
Koregaon Park	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
Lashkar	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1
Wakad	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Hinjewadi	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
Pimpari	2	0	0	1	1	1	0	0	0	0	0	0	2	0	0	1	1	1
Chinchwad	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
Nigadi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bhosari	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIDC Bhosari	NA	0	0	0	0	1	NA	0	0	0	0	0	NA	0	0	0	0	1
Sangavi	0	2	1	0	0	3	0	2	1	0	0	0	0	0	0	0	0	0
Cyber Cell	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cybercrime in Pune	**3**	**5**	**5**	**5**	**5**	**16**	**1**	**5**	**4**	**1**	**1**	**4**	**2**	**0**	**1**	**4**	**4**	**8**

`

Table 32: Summary of Yearwise Cyber Crimes under Section 67 Registered, Resolved and Pending in Pune City during 2011-2016

Cyber Crimes	2011	2012	2013	2014	2015	2016
Registered	3	5	5	5	5	16
Resolved	1	5	4	1	1	4
Pending	2	0	1	4	4	8

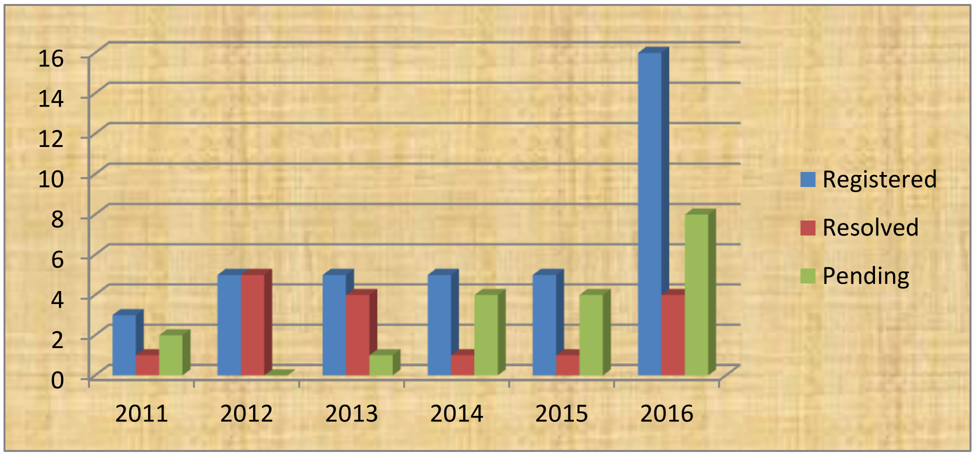


Figure 20: Cyber Crimes under Section 67 (2011-2016)

INFERENCE:

1) There is significance rise in cyber crimes under Section 66 of IT Act from 2011-2016. In last 5 years, cyber crimes increased 4 times as compared to 2011.
2) The percentage of crimes resolved is between 20-45% and percentages of pending crimes are 72-85% which is a matter of serious concern.

4.6 –The Cyber safety Awareness amongst Internet users of age group (18-30 years and above 30 years) in Pune city

Survey: Survey of "Cyber Safety Awareness" was conducted for the age group of 18-30 years and above 30 years.

Objective: The objective of this survey is to find out the facts /reasons why cyber crimes are increasing at rapid speed in last 5 years (2011-2015).

Reasons: Various reports on Cyber crimes reveals that Cyber crimes are increasing at an alarming Rate in last 10 years.

Instances of cyber-crimes have gone up by 207% in the last one year from 2014 to 2015. With the World Wide Web, cyber-crimes are on the rise. Credit card frauds, phishing email scams, online romance scams, hacking of accounts and revenge cases are some of the more notorious forms of cyber-crimes. There are even cases of matrimonial fraud in the online portals. People started believing relationships of virtual world.

In such a changed scenario, digital evidence is needed in almost all legal cases today. The evidence is mostly in the form of e-mails, WhatsApp messages and social media chats.

It is significant to note that data theft is also on the rise, where databases of major E-commerce Companies , firms are targeted and subsequently the user data is used to commit online banking frauds, extortion etc.

Cyber crimes in Maharashtra are highest as compared to other states of India (refer Chapter 4-4.2 and 4.3). Cyber crimes in Pune City are greater in no. as compared to other cities in Maharashtra. Therefore conducting this survey is most important from research point of view. Survey of approximately 1122 people of age group between 18-30 years and above 30 years was conducted. This age group is selected as per National Crime Records Bureau of India. They have categorized crimes in 4 age categories –a) 18-30 years b) 30-45 years c) 45-60 years d) 60 and above 60 years.

The highest number of cyber crimes are committed by persons of the age group of 18-30 years.

References 1,2 ,3: Reports from NCRB on cyber crimes for the year 2009-2015

Sample Size: 1122

Sample Type: People from various graduation Streams such as Arts, Commerce, Science, Engineering, Computer, B.Tech., Agriculture as well as working professionals and senior citizens have been selected for Survey on cyber safety awareness.

`

Objective: The objective of this survey is to find out the facts /reasons why cyber crimes are increasing at rapid speed in last 10 years.

The data is collected from 1122 people by distributing Questionnaire which was later on computerized using Google forms. This data then processed using SPSS-20 software for analytical study.

Table 33: Respondents having an email account (age 18-30 years)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	1065	94.9	94.9	94.9
	No	57	5.1	5.1	100.0
	Total	1122	100.0	100.0	

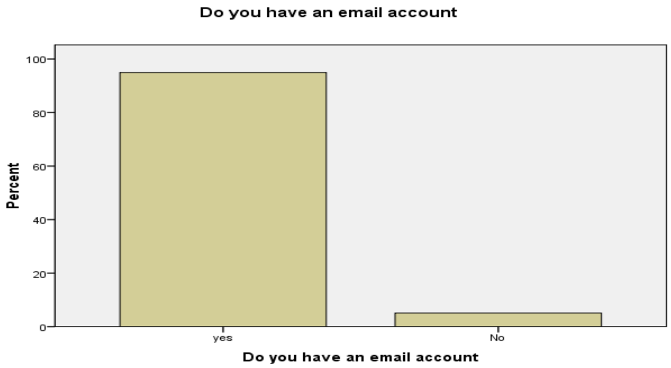


Figure 21: Survey of respondents having Email account

INFERENCE: Out of 1122 people, 1065 are Internet users and 57 are non internet users. Perdcentage of Internet users is 94.9%. The next question asked to these users is whether their password is strong.

`

Table 34: Respondents survey for strong password

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Alphabet	267	23.8	23.8	23.8
Number	176	15.7	15.7	39.5
Special characters	27	2.4	2.4	41.9
Alpha numeric	261	23.3	23.3	65.2
Combination of all	391	34.8	34.8	100.0
Total	**1122**	**100.0**	**100.0**	

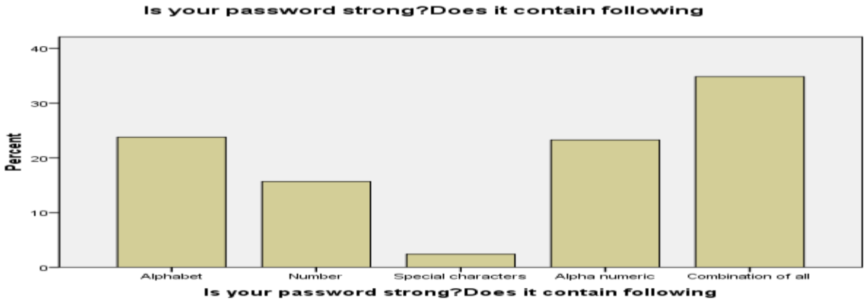


Figure 22: Strong password survey

INFERENCE:

23.8% people are using only Alphabets, 15.7% people are using only Number, 2.4 % people are using Special characters, 23.3 people have alphanumeric password whereas 34.8 are using Combination of alphabets, Numbers, Special characters. Strong password cannot be easily hacked by Hackers. Hence from above population, 34.8 people have strong password and rest population i.e. 65.2% people do not have it which is a serious threat. There are chances that their passwords can be easily guessed, hacked or altered which will give rise to cyber crimes. The cyber crimes occur through Social Networking sites. So users of it were identified using the following questions.

`

Table 35: Social networking sites used by respondents

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid facebook	529	47.1	47.1	47.1
twitter	40	3.6	3.6	50.7
whatsApp	436	38.9	38.9	89.6
any other	60	5.3	5.3	94.9
nothing	57	5.1	5.1	100.0
Total	1122	100.0	100.0	

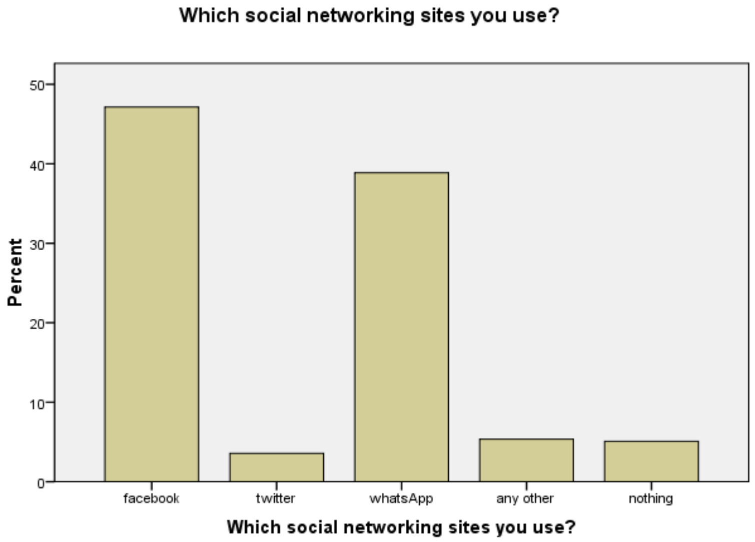


Figure 23: Use of Social Networking sites

INFERENCE: Out of 1122 users, Facebook users are 47.1, Twitter users are 3.6, WhatsAppusersare38.9% and others are 5.3% . Only 5.1% people are not using any social media. Hence the probability of committing cyber crimes by users on social networking sites is more.

`

Table 36 : Different password for email and social media accounts

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	819	73.0	73.0	73.0
	no	303	27.0	27.0	100.0
	Total	1122	100.0	100.0	

INFERENCE: The above table shows that 73% people have different password for their social accounts. Having same password for many accounts may help hackers to hack multiple accounts easily which is a threat. This may lead to economic frauds, defamation, stealing of personal or organizational information etc. 27% people have same passwords for their different accounts. This group may fall victim to cyber crime.

Going ahead, Uploading personal details such as photographs, contact nos. on social networking sites can help hackers to steal identity of individual or organization. They may send messages on emails for getting bank account details, personal information, SMS on mobile for discounts, offers, lottery, lucky draw etc. which may be termed as Nigeria Fraud.

Table 37: Respondents having uploaded following personal details on social networking sites?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Your photo	326	29.1	29.1	29.1
	contact no.	35	3.1	3.1	32.2
	Email	163	14.5	14.5	46.7
	Address	12	1.1	1.1	47.8
	All	432	38.5	38.5	86.3
	Nothing	154	13.7	13.7	100.0
	Total	1122	100.0	100.0	

`

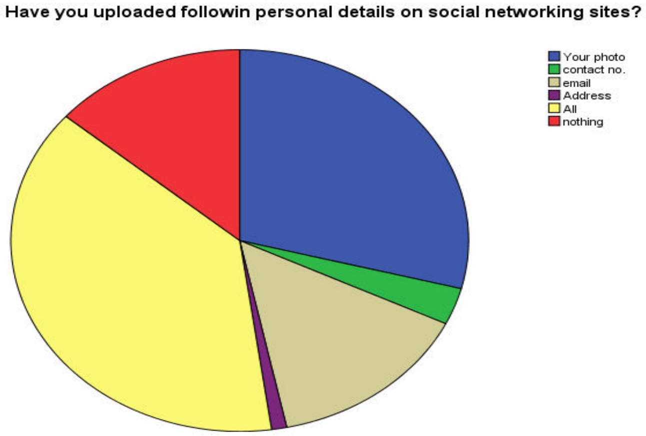


Figure 24: Various details uploaded on Social Networking sites

INFERENCE: The above table shows that out of 100, 29 % people are uploading their photographs, 3.1 % people are uploading Contact numbers, 14.5% are uploading email-ids, 1.1% people are uploading their addresses on social networking sites which is a serious threat and may lead to cyber crimes.

Table 38: Accepting unknown friend's request

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	53	4.7	4.7	4.7
	no	815	72.6	72.6	77.4
	sometimes	254	22.6	22.6	100.0
	Total	1122	100.0	100.0	

INFERENCE:

Out of 100%, 4.7 % people accept unknown friend’s request. 22.6 % people sometimes accept such requests. Total 27.3% people use unknown friend’s request. This percentage is significant as they may indirectly providing personal information and will be at risk.

`

Table 39: Installing antivirus software on PC

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes	858	76.5	76.5	76.5
no	264	23.5	23.5	100.0
Total	1122	100.0	100.0	

INFERENCE:

1) 23.5 % respondents have said that they have not installed Antivirus software on their PCs.

2) This may lead to data loss or loss of personal or business information.

3 These percentages are significant and shows there lack of cyber safety or information security awareness which is a risk.

Table 40: Installation of antivirus and firewall on PC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	installed antivirus only	509	45.4	45.4	45.4
	installed firewall only	35	3.1	3.1	48.5
	installed both-antivirus & firewall	344	30.7	30.7	79.1
	installed none	234	20.9	20.9	100.0
	Total	1122	100.0	100.0	

`

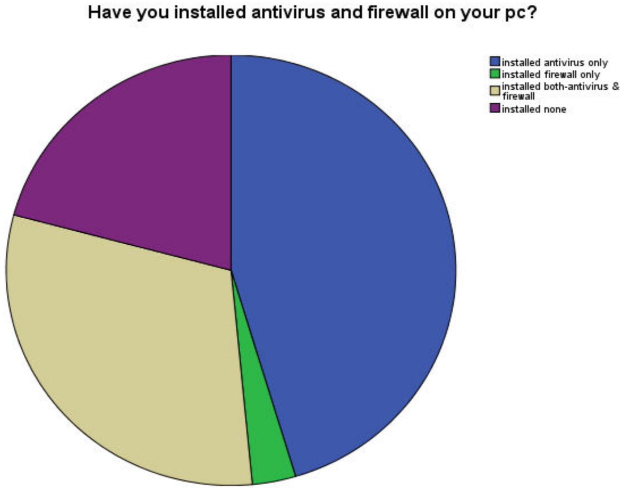


Figure 25: Installation of antivirus and firewall on PC

INFERENCE:

Going ahead, along with antivirus very few people have installed Firewall i.e. 30.9%. This percentage is very low and showing that almost 70% people need to make tight security for their PCs to avoid future risks.

Table 41: People who purchased licensed software for their PC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	580	51.7	51.7	51.7
	no	542	48.3	48.3	100.0
	Total	1122	100.0	100.0	

Again, many people install pirated softwares. 48.3% people have not used authenticated softwares for their PCs. This is a risk for falling victim to data loss. More and more awareness on using original software licenses to be created by companies and cyber cells.

`

INFERENCE:

Above table shows that 30% people are not taking back up of their sensitive and important information. This may lead to personal data loss, loss of organizations data and in turn loss in business. This also leads to risk of cyber crimes.

Table 42: People taking Backup of sensitive and important information

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**Yes**	**785**	**70.0**	**70.0**	**70.0**
	No	**337**	**30.0**	**30.0**	**100.0**
	Total	**1122**	**100.0**	**100.0**	

Table 43: People using UPS for data backup

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	451	40.2	40.2	40.2
	no	671	59.8	59.8	100.0
	Total	1122	100.0	100.0	

INFERENCE:

Above table shows that 59.8% people are not using UPS. In case of power failure data may be lost.

`

Table 44: People's awareness on IMEI of mobile

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	479	42.7	42.7	42.7
	no	643	57.3	57.3	100.0
	Total	1122	100.0	100.0	

INFERENCE:

57.3% People are not aware about IMEI no. of Mobile. In case of Mobile loss, this data is required. Otherwise the data from mobile be stolen and can be misused in case of Mobile theft.

Table 45: People shopping on reputed website

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	643	57.3	57.3	57.3
	No	479	42.7	42.7	100.0
	Total	1122	100.0	100.0	

INFERENCE

There are 57.3% people shopping on website. Hence the rules of online safety must be known.

Table 46: Tendency to discard receipts after ATM transaction

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	802	71.5	71.5	71.5
	no	320	28.5	28.5	100.0
	Total	1122	100.0	100.0	

`

INFERENCE:

As far as banking transactions are concerned most of the people are using ATMs for money withdrawals. It has been observed that 71.5% people discard ATM receipts after transaction. This gives space for cyber criminals to know the balance, account details of that person. He may misuse the account for money withdrawal by making duplicate ATM card.

Table 47: Noting down ATM card and customer service no. on their mobile

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	759	67.6	67.6	67.6
	no	363	32.4	32.4	100.0
	Total	1122	100.0	100.0	

INFERENCE:

Many people have a habit to note down their ATM card no. and Customer service number in their mobile as contact no. When mobiles are lost such confidential information is hacked by hackers and misused for personal gains. Here after survey, we came to know that 67.6% people are doing this practice and hence may become victim of cyber crimes.

Table 48: Habit of Proper log out after using email account and internet banking services

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	962	85.7	85.7	85.7
	no	160	14.3	14.3	100.0
	To9al	1122	100.0	100.0	

`

INFERENCE:

People nowadays use internet and do online banking transactions for ease. Sometimes they forget to proper log out from the current account. This percentage here is 14.3% though seems less, may be risky to that group of people who do this knowingly or unknowingly. This may lead to attending your open accounts by some hackers who are always get benefit of people's ignorance.

Table 49: Tendency to store password, PIN in mobile as contact no.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	258	23.0	23.0	23.0
	no	864	77.0	77.0	100.0
	Total	1122	100.0	100.0	

INFERENCE: Many people have a habit to note down their password or PIN (Personal Identification Number) in their mobile devices as contact no. When mobiles are lost, such confidential information is hacked by hackers and misused for personal gains. Here after survey, we came to know that 23% people are doing this practice and hence may become victim of cyber crimes

Table 50: People who receive email /SMSs / phone calls that promise large sum of money / discounts

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	596	53.1	53.1	53.1
	no	526	46.9	46.9	100.0
	Total	1122	100.0	100.0	

`

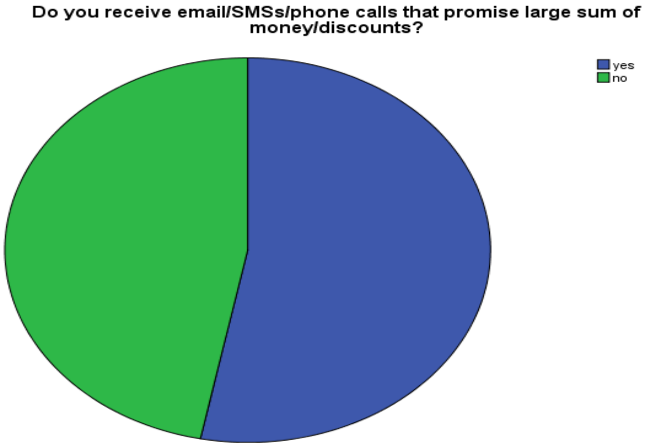


Figure 26: People who receive email/SMSs/phone calls that promise large sum of money/discounts

INFERENCE:

53.1% people are saying that they are getting such calls that promise large sums of money/discounts. Hackers nowadays find out smart ways to trap people by promising gifts, discounts, offers or pretending that they are people from Bank.

Table 51: People responding to email /SMSs /phone calls

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	149	13.3	13.3	13.3
	no	973	86.7	86.7	100.0
	Total	1122	100.0	100.0	

`

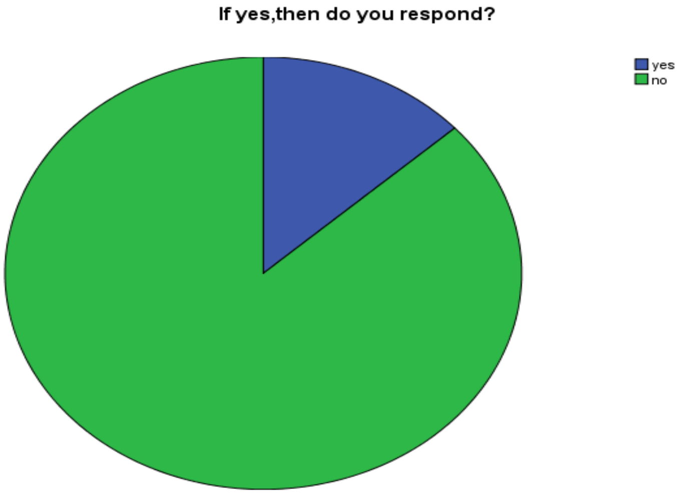


Figure 27: People responding to email /SMSs / phone calls

INFERENCE:

13.3 % people are saying that they are responding to such calls. Though such percentage seems low, in future the percentage to call people may increase if 'Awareness on cyber safety' is not created.

Table 52: Way of responding to unknown calls

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	By replying to SMS/email	130	11.6	11.6	11.6
	By calling contact no. given in email/sms	60	5.3	5.3	16.9
	By entertaining their call	76	6.8	6.8	23.7
	not applicable	856	76.3	76.3	100.0
	Total	1122	100.0	100.0	

`

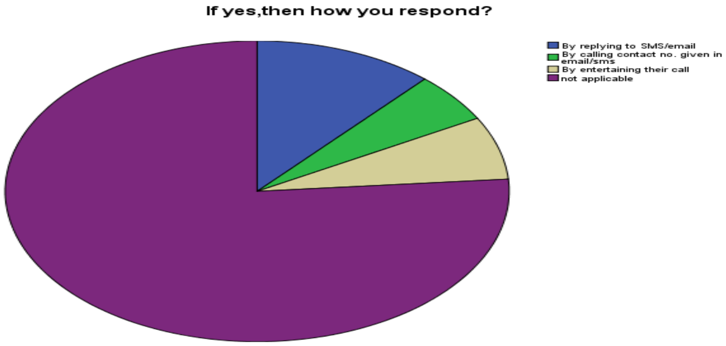


Figure 28: Way of responding to unknown calls

INFERENCE:

People respond to unknown calls in different ways. 11.6 % people respond By replying to SMS/email, 5.3% people respond by calling on contact no. given in email/ sms, 6.8% people respond by entertaining their call. Total 23.7% people respond by any means which is a matter of serious concern.

Table 53: Percentage of uploading following personal details on social networking sites

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Your photo	326	29.1	29.1	29.1
	contact no.	35	3.1	3.1	32.2
	email	163	14.5	14.5	46.7
	Address	12	1.1	1.1	47.8
	All	432	38.5	38.5	86.3
	nothing	154	13.7	13.7	100.0
	Total	1122	100.0	100.0	

`

INFERENCE:

1) From Table 53, it may be inferred that 38.5% people are uploading all the details which is of serious concern as others may misuse the information.

2) 29.1% people are uploading their photos which gives identity proof for cyber criminals.14.5 % people are giving their email ids.

3) Only 13.7 % people are giving no details means remaining 87.3% are giving their personal information in different ways online. So cyber criminals are looking for such type of data which may carry risk of cyber crimes

Table 54: People knowing types of cyber crimes

	Type of cyber crime	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nigerian Fraud	7	.6	.6	.6
	Credit Card Fraud	124	11.1	11.1	11.7
	Phishing	30	2.7	2.7	14.3
	Identify Theft	64	5.7	5.7	20.1
	Hacking	435	38.8	38.8	58.8
	All above	368	32.8	32.8	91.6
	None	94	8.4	8.4	100.0
	Total	1122	100.0	100.0	

INFERENCE:

From Table no. 55, it may be inferred that

1) Only 0.6% people have heard about Nigerian fraud.11.1% people know about Credit card fraud.2.7% people know about phishing crimes. 5.7% people know about Identity theft.38.8% people know about Hacking.

2) Only 32.8% from above respondents know something about few cyber crimes. This shows that there is a need to create awareness about **Cyber safety and cyber crimes** amongst the people.

`

Table 55: People using Technologies

Technology Type	Users	Not used
Email Account Users	94.91%	5.09%
People connected with Social Networking sites	43%	57%
Antivirus installed	76.5	23.5
Shopping on reputed website	57.3	42.7
Use of Debit Credit cards for financial transactions	60%	40%

INFERENCE:

The above Table shows that people are now making use of various technologies for communication and other tasks such as Social networking sites, financial transactions through Debit and credit cards, online shopping. These percentages are significant and indicative that these people must know the safety rules while online or on social indicative that these people must kno the safety rules hile online or on social networking sites.

`

Table 56: Vulnerability Gateways observed from Questionnaire 2

Sr. No.	Vulnerability Gateways for cyber crimes (How it may happen)	Yes	No	Threat	Risk level (H/ L/M)	Possibility of Cyber crimes
1	Frequency of Changing password	40.19%	59.81 %	Anyone can guess password. Data can be stolen.	H	H
2	Strong password	34.8%	65.2%	Majority of the users (65%) do not have strong password.	H	H
3	Change of password tendency	40.2%	59.8%	Almost 60% Users are not changing passwords. This may lead to threat to their accounts by Hackers.	H	H
2	Different passwords for email and social networking accounts	73%	27%	Good to have different passwords. But People may forget passwords. If stored on mobile or database it may be hacked. 27 % people are using same passwords which is risk to their social networking accounts	H	H
3	Accepting Unknown Friends Requests	27.3%	72.6%	Carry risk of personal and social life.	H	H
4	Antivirus Software installed on PC	76.5%	23.5%	Good awareness. Still 23.5% people are not using Antivirus. This may result in data loss due to virus intrusion.	H	H
5	Using Licensed Antivirus software	51.7%	48.3%	Almost 49% users are using pirated software which is not correct.	H	H
6	Installing Antivirus and Firewall both	30.7%	69.3%	Need to create awareness amongst 70% people about use of Firewall.	H	H
7	Internet WI-FI password secure	75.7%	24.3%		L	L
8	Back up of sensitive information	70%	30%	Chance of information / data loss	M	M
9	UPS for backup	40.2%	59.8%	Chances of Information /data loss	H	H
10	Knowing IMEI of your mobile	42.7%	57.3%	Helps in Mobile theft. Not knowing IMEI may lead to hack personal information/ Financial loss.	H	H
11	Debit/Credit card users	63.3%	36.7%	Use of cards increases risk of using it carefully.	H	H
12	Online Shopping on reputed websites	57.3%	42.7%	Threats through online shopping increases if not used properly	H	H
13	Discarding receipts after ATM transactions	71.5%	28.5%	Details of transaction may be used by hackers.	H	H

`

14	'Log out' after using email-Account & Internet Banking services	85.7%	14.3%	Leaving account without logging off are the entry points for hackers/cyber criminals.	**M**	**M**
15	Storing PIN on mobile as contact no.	23%	77%	In case of mobile theft, details are used by cyber criminals.	**M**	**M**
16	Bluetooth on	15.2%	84.8%	Chances of data , file transfer increases	**M**	**M**
17	Receiving Emails/SMSs/ Phone calls that promise large sums of money /discounts	53.1%	46.9%	Gateways for cyber crimes of responded	**H**	**H**
18	Responding to such calls	13.3%	86.7%	Inviting the cyber criminals by accepting such calls	**M**	**M**
19	Uploading personal details on Social websites	47.8%	52.2%	May lead to personal/Financial/Social loss	**H**	**H**
20	Way of responding to calls (by SMS/Email/Call/entertain such calls)	23.7%	76.35 %	Risk of cyber crimes increases	**M**	**M**
21	Accepting unknown friend's request	27.3%	72.7%	Risk of cyber crimes increases	**H**	**H**
22	**Awareness about terms**					
a)	Nigerian Frauds	0.6%	99.4%	Very less awareness may lead to Cyber crimes.	**H**	**H**
b)	Credit card frauds	11.1%	88.95 %		**H**	**H**
c)	Phishing	2.7%	98.3%		**H**	**H**
d)	Identity Theft	5.7%	94.3%		**H**	**H**
e)	Hacking	38.8%	61.2%		**H**	**H**
f)	All above	32.8%	67.2%		**H**	**H**

* (Note: Yellow mark highlights Risk Level High, Low, Medium)

The above Table shows that people are now making use of various technologies for communication and other tasks such as Social networking sites, financial transactions through Debit and credit cards, online shopping. These percentages are significant and indicative that these people must know the safety rules while online or on social networking sites.

`

INFERENCE:

1) Almost 95% people use Internet and emails.43% people are using Social networking sites such as WhatsApp, Facebook and Twitter. So they are more prone for falling victim to cyber crimes.
2) 76.5 % people are using Antivirus software. Awareness of Using Antivirus software is good. Still 23.5 % educated group is not using antivirus which may lead to fear of Information Security or Data security.
3) Almost 57.3 % people are shopping online. This percentage may rise in future. Therefore risk of cyber crimes (sending Personal information, money risk) is also increased. Debit /Credit card users at this age group (mostly students) are 60%. The risk associated with loss of cards, careless ATM or online transactions may lead to cybercrimes.

Conclusion of data analyzed from Questionnaire 2

1) Observations on ‘Technology awareness’ and ‘Cyber Security Risk Analysis Report’ between the age group of 18-30 years based on survey in Pune region reveals that there is great need to conduct ‘Proactive Awareness Campaign’ on ‘Cyber Safety’.
2) Though people are using new technologies such as Internet, Emails, Social networking sites , antivirus, online shopping, Debit/Credit cards for financial transactions, they are less aware about do’s and don’ts of using these technologies which is a serious threat to increase cyber crimes.
3) There is need to inculcate ‘Best Practices’ amongst this age group so as to reduce quantum of cyber crimes.
4) If awareness is not created, the rate of cyber crimes will increase which in turn will create burden on ‘Cyber Cell’ and ‘Cyber Forensic labs’.

   This will affect the effective investigation of cyber crimes in Pune region. The period to resolve registered cyber crimes will increase which is boon for Cyber criminals.

`

4.7 –Analysis of the Problems faced by Cyber Cells, Police stations in Pune city during cyber crime Investigation Process

Table 57:Problems faced by Pune Police stations during Cyber crime investigation

		DIVISIONS														
		Chatush-rungi		Pimpri	Khadaki				VishramBaug		Swargate			Lashkar		
Sr. No.	**Questionnaire 4 (Options Yes=1, No=0)**	**Wakad**	**Hinjewadi**	**Bhosari**	**Yerawada**	**Khadaki**	**Dighi**	**Chandan Nagar**	**Shivajinagar**	**Vishrambaug**	**Bibwewadi**	**Sahkarnagar**	**Swargate**	**Bundgarden**	**Total - No**	**Total - Yes**
1	Is there any special Department/ Cyber Cell in your Police station?	0	0	1	1	1	0	0	1	1	0	0	1	0	7	6
2	Is there sufficient manpower recruited for handling the Cyber Cases in Police Station?	0	1	1	1	0	1	1	0	0	0	0	0	0	8	5
3	Is there training given to staff by Govt. on cyber crime investigation?	1	1	1	1	1	1	0	0	0	1	1	1	0	4	13
4	Is this staff handles Cyber Cases only ?	0	0	0	0	0	0	0	0	0	0	0	1	0	12	1
4.1	Have they allotted some other work other than Cyber Cases (please specify)	1	1	1	1	1	1	1	1	1	1	1	1	1	0	13
5	Is the Cyber Cell Well Equipped in all aspects?	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0
6	Is the Cyber Cell using the latest S/W ? Please specify the name of the S/W & version	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0
7	Is the Cyber Cell using the latest hardware ?	0	0	0	0	0	1	0	0	0	0	0	0	0	12	1
8	Do you get CDR from ISPs in time?	1	0	0	0	0	1	0	0	0	0	0	0	0	11	2
9	Do you face any problem in investigation if the person handles the case, get transferred to other location?	0	0	1	1	1	0	0	1	1	1	1	0	1	5	8
10	Do you have the authority/powers to resolve the Cyber Crime?	0	0	0	0	0	1	1	1	1	1	1	0	1	6	7
11	Do you take support of External agencies/Experts to resolve cyber Crimes?	1	1	0	0	1	1	0	0	0	1	1	1	0	6	7
12	In case of International Cyber crimes, do you get support from foreign countries?	0	0	0	1	0	0	N.A.	0	0	0	0	0	0	12	1

`

INFERENCES: From the above table it may be inferred that

1) Only 46% police stations have Special Cyber Cells for cyber crime investigation.
2) There are only 38% police stations where there is sufficient man power.
3) Out of theses police stations 92% police stations are saying that there is no dedicated manpower. The staff is sent to other duties as and when required. So there is no dedicated or special staff for cyber crime investigation.
4) Only 30 % police stations are saying that they are not getting training on cyber crimes.
5) 100% Police stations are saying that, they do not have well equipped Cyber Cell.
6) 100% Police stations are saying that they are not using latest Hardware.
7) 100% Police stations are saying that they are not using latest Software.
8) 82%Police stations are not getting CDR from Internet Service Providers (ISPs).
9) 38 % Officers are saying that they are facing problems when person handling cyber crime case gets transferred to other locations.
10) 46%Police officers are saying that they do not have the authority to resolve cyber crimes.
11) 46% Police officers are saying that they take support of external agencies for cyber crime investigation.
12) 92% Police officers are saying that they are not getting support from foreign countries in case of investigation of International cyber crimes.

The above information given by all Senior APIs, DCPs based on their experience and problems they faced during investigation. Hence it is more reliable.

Based on the above inferences, the f**actors affecting effective investigation of cyber crimes** are as follows:

1) Lack of Special cyber cell.
2) Lack of dedicated and trained manpower.
3) Lack of latest hardware and software for cyber crime investigation.
4) No Frequent training for cyber crime investigation.
5) Timely Response from ISPs is lacking.
6) Lack of support of foreign countries while investigation of international cyber crimes.

Table 58: Problems faced by cyber crime Investigation Officers of Pune region and their valuable suggestions for speedy investigation of cyber crimes

Various police stations have given written feedback on the problems faced by them during cyber crime investigation and all of them had given valuable feedback based on their experience on cyber crime investigation.

Sr. No	Divisions Police Station	Problems faced by Cyber Crime Investigation Officers / ACP / DCP of Pune region	Valuable Suggestions from them to speed up Cyber Crime investigation process
1	**Khadaki** Chandan Nagar Dighi	1) Support of external agencies /experts for Cyber Crime Investigation not easily available 2) No Support from Foreign Countries in case of International Cyber Crime.	1. Technical Staff should be furnished to each Police Station 2. There is Urgent need to set up separate Cyber Police Station with sufficient and trained officers & staff with proper software & Hardware. 3. Power of Investigation to be given to PSI/API 4. Cyber Crime is virtual. At present, offence is registered where the complainant is residing. 5. After investigation/enquiry it is found that accused have committed the Cyber Crime out of state. It is not feasible every time to send team to nab the culprit. So, it is better to make preliminary enquiry by the police station where complainant is residing and registered FIR under zero & send to concern police station where accused have committed act of crime.
2	**Chatushrungi** Wakad Hinjewadi	3) The training is given to staff by Govt. on Cyber Crime but only theory is taught & no practical exposure of Cyber Crime Investigation. 4) Due to lack of awareness about Cyber safety, people give confidential information to unknown person. 5) Banks are not co-operating for investigation of ATM frauds. 6) Job frauds are increasing because of lack of awareness of complainant.	6. To avoid ATM frauds, bio-metric thumb should be used for ATM transactions

`

4	**Pimpri** Bhosari	7) Police stations are facing problems while investigation of social networking crimes,Credit/Debit/ATM/Insurance /Job/Loan/Matrimonial/Online business frauds,hacking[mail, website data] & Mobile Offences. 8) No Authority to communicate directly to Companies [ISPs] 9) Late Response from ISPs,Bank etc.	
6	**Vishrambaug** Shivajinagar, Vishrambaug	10) Investigation process is delayed as companies related to social networking crimes are not providing information in time. 11) Information required from other concern police stations related to cyber crimes [Credit/Debit/ATM/Insurance /Job/Loan/Matrimonial/Online business fraud] not getting in time. 12) If the investigation officer transferred to other location, investigation process is affected.	
7	**Swargate** Bibwewadi, Sahakarnagar	13) Social Networking Crimes (facebook ,Twitter, other sites)- All the above sites do not have their legal support office in India,so the offices of these Companies are communicated via e-mail & needs to wait till their response, which delays investigation process. 14) There is no problem of investigation of Credit/Debit/ATM/Insurance /Job/Loan/Online business fraud till the complainant is not late for registering complaint. 15) Do not get log in details from Banks. 16) Do not get details of web page & page construction details. 17) Hacking [mail, website, data] &Mobile Offences- There is no technical team to help in investigation of hacking	7. Designated IO [Investigation Officer] in IT act is Police Inspector. As Cyber Crimes are increasing, designated officer [IO] should be at least API. 8. There should be specialization in handling cyber crime like separate ‘Cyber Police Station’.

		offences ,the complainant is suggested to contact cyber cell. 18) Do not get log in details from ISPs. In case of Mobile offences no prompt response from Service Providers. Only Nodal Officer is authorize to get information.PI incharge must get power to communicate directly. 19) Matrimonial Fraud-Do not get details of IP address from ISP. 20) Legal Issues- There should be frequent training about seizing & packing of digital evidence.	
8	<u>**Lashkar**</u> Bund Garden	21) Information required from other concern police stations related to cyber crimes (Credit/Debit/ATM/Insurance/Job/Loan/Matrimonial/Online business fraud] not getting in time. 22) Social Networking Crimes (facebook ,Twitter, other sites)- Investigation process is delayed as companies related to social networking crimes are not providing information in time.	

The problems mentioned above and suggestions given by them are of utmost importance and must be solved with the help of Government authorities.

4.8 – Need of Cyber Safety Awareness for school children below age group of 18 years

The cyber crimes identified between age group of 18-30 years are highest as per the reports of NCRB. It highlights that the Cyber safety awareness survey conducted for the age group of 18-30 years showed lack of awareness in following.

This shows that Awareness needs to be created not only for this age group but age group of school children above 11.

The researcher got the opportunity to work with Quick Heal Foundation of Quick Heal Technologies which is a dominant name for Data and Network Security. Company is doing research and development for combating new viruses. Cyber security is one of the initiatives of Company under CSR (Corporate Social Responsibility). At present researcher is working as 'Chairman-Cyber Awareness Literacy cell' of Maharashtra region of Quick Heal Foundation. This helped researcher to reach school Children of Pune city. Researcher approached various schools in Pune city. Researcher through her college conducted active initiative to spread Cyber security Awareness Campaign amongst various schools of Pune city.

For this, team of Quick Heal prepared presentation. They trained students for delivering presentation which is based on current cyber crimes on FaceBook, Social media, Nigerian frauds Phishing etc.. Audio and Video presentation made it attractive. School children and teachers liked this presentation very much which is evident from the reports collected from every school.

The brief of this campaign:

Schools approached	**: 76**
Children sensitized	**: 49,372**

`

"CYBER SECURITY AWARENESS CAMPAIGN" CONDUCTED FOR SCHOOL CHILDREN (STD. 5TH to 10TH)

Table 59: Cyber Security Campaign for School Children

Std.	5th	6th	7th	8th	9th	10th	Total
Students	8432	8431	9264	10239	6849	6157	49372

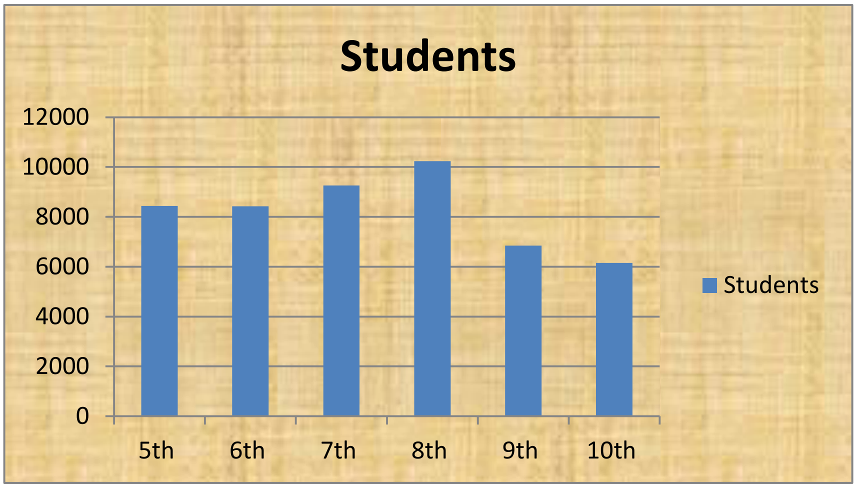


Figure 29: Cyber Security Campaign for School Children

Presentation Feedback:

From 76 schools, 168 divisions from std. 5th to std. 10th reached.

Feedback received from every school is encouraging and emphasis this type of awareness session cyber safety for their school children.

`

Feedback From Various Divisions On Cyber Safety Awareness

Table 60: Total Divisions Approached for Cyber safety Awareness

	Feedback from various divisions				
Total Divisions	Excellent	Better	Very Good	Good	Satisfactory
168	106	7	1	52	1

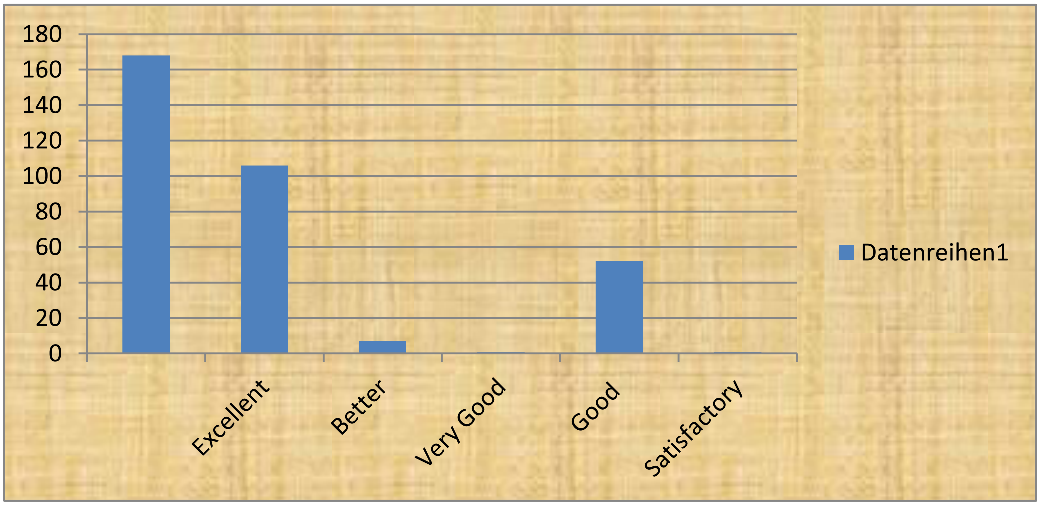


Figure 30: Total Divisions Approached for Cyber safety Awareness

INFERENCE:

1 Above feedback shows that Cyber Safety Awareness Campaign conducted in Schools for students of age group below 18 years.

2 This campaign was conducted by the students of age group above 18 years.

3 Feedback of 108 schools was excellent, 7 schools better and 52 schools was good. It was appreciated by the Children, Teachers and School Principals.

`

Remark/Suggestions from School Principals/Teachers:

Remark/Suggestions obtained from School Principals/Teachers are compiled.

Table 61: Unique Suggestions from various school Principals/Teachers

Sr.No	**Suggestions / Remarks**
1	Good activity. Useful for students.
2	Informative Seminar. Useful for creating Responsible Citizen
3	Necessary to know cyber crime.
4	Story on cyber crime through PPT should be more effective.
5	Would like more such lectures on different topics in future.
6	Interesting story on cyber crimes.
7	Presentation excellent & helpful
8	Will suggest to do these sessions/ activity frequently.
9	Useful for children of this age.
10	We got a lot of information about cybercrime and mobile use
11	Useful for children of this age.
12	Explanation in Marathi would be more preferable.
13	Translate English words related to Cyber crimes in Marathi.
14	Cyber safety awareness program is very necessary. Nice team work. Helpful to students
15	Presentation Informative. This is a kind of social initiative and useful to Teachers also.
16	Information give awareness about disadvantages of online chatting & social site
17	Much needed program, will create awareness amongst students
18	Cyber safety awareness is the need of an hour.
19	Awareness created in students is helpful
20	Session will really create awareness amongst students. Considering the present age of School children this is a burning issue.
21	More examples related to students should be given.
22	Like the story form of explaining an important issue
23	Appealing presentation, besides these problems other problems related to cyber crimes should be presented.
24	More stress should be on precautions while using social media sites and while surfing on the internet.
25	Attractive and influencing presentation. More Consequences of cyber crimes Needs to be discussed.
26	Need to discuss more on impact of cyber crimes
27	Cyber Safety Awareness program is useful for 11th and 12th Standard students because they are teenagers.
28	Children would understand the consequences of Chatting on face book with strangers.
29	Video can be used or real life examples can be given.
30	Your students must visit our school every year.

`

This Campaign highlights the following facts.

1) Survey of this type is essential in the society.
2) Children of this age group are receptive and can understand and take care while handling Internet, Social media, Facebook, and other technologies such as ATMs, Mobiles etc. if made aware of the consequences of Cyber crimes.
3) As students of Colleges are trained for this campaign, they get automatically acquainted with this issue. Hence students of age group of 18 years and above were also covered under this 'Cyber Safety Awareness Campaign'.
4) Formation of 'Cyber Awareness Literacy Cell' in Schools and Colleges will help to form Cyber literate society.

4.9 – Cyber Security Risk Assessment Matrix based on results of points 4.2 - 4.8

Risk assessment:

It is a step in a procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard). Quantitative risk assessment requires calculations of two components of risk(R), the magnitude of the potential loss (L), and the probability (p) that the loss will occur.

We are specially studying Risk assessment with reference to cyber security. This will help in analyzing factors affecting effective investigation of cyber crimes. There are two types of Risk Assessments·

1) Quantitative Risk Assessment
2) Qualitative Risk assessment

1) Quantitative Risk Assessment :

- Quantitative risk assessments include a calculation of the 'Single Loss Expectancy (SLE)' of an asset.

- The single loss expectancy can be defined as the loss of value to asset based on a single security incident.
- The team then calculates the 'Annualized Rate of Occurrence (ARO)' of the threat to the asset. The ARO is an estimate based on the data of how often a threat would be successful in exploiting vulnerability. From this information, the Annualized Loss Expectancy (ALE) can be calculated.

2) Qualitative Risk assessment :

- **Qualitative risk assessment** comes into play when we have the ability to map an amount to a specific risk.
- Qualitative Risk assessment assumes that there is already a great degree of uncertainty in the likelihood and impact values and defines them, thus risk, in somewhat subjective or qualitative term.
- Qualitative Risk assessment typically give risk results of 'High', 'Moderate' and 'Low'. By providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization.

Table 62: Risk Assessment Matrix

RISK ASSESSMENT MATRIX			
	H/M/L	H/M/L	H/M/L
MOTIVATION	HIGH	HIGH	LOW
CAPABILITY	HIGH	HIGH	MODERATE
CONTROLS	LOW	MODERATE	HIGH
RISK LEVEL	HIGH	MODERATE	LOW

(P.N. above Risk Assessment Matrix is as per Microsoft's Information Security Standards)

After studying cyber crime scenario and various other factors through different questionnaires, following **Risk Matrix** is prepared. This Risk matrix shows Risk levels before and after implementing security measures or Controls.

`

Table 63: Study showing Risk levels before and after applying security controls

FACTOR	Volume/ Quantum	RISK LEVEL (Before)	Controls Impleme-nted	RISK LEVEL (After)
The Cyber crimes in India (2009-2016)	High	High	High	Low
The cyber crimes in Maharashtra (2011-2016)	High	High	High	Low
The cyber crimes in Pune city and PCMC (2011-2016)	High	High	High	Low
Cyber Safety Awareness amongst Internet users in Pune	Low	High	High	High
Problems faced by cyber cells, cyber forensic labs, police stations in Pune during cyber crime investigation	High	High	High	Low
Need of awareness in school children below age 18 years	High	High	High	Low

INFERENCE:

1) Above risk matrix shows the degree of Risk is High as far as quantum of cyber crimes in India, Maharashtra, Pune city and PCMC. This risk level is high because the controls implemented are low. Therefore there is need of high Security control to avoid increasing cyber crimes.
2) Problems faced by cyber cell, cyber forensic labs, Police stations during cyber crime investigation are high. If their problems are tackled by supplying adequate man power, necessary hardware and software required for cyber crime investigation, timely help of ISPs and law enforcement agencies for crime investigation then they will face minimum or no problem during investigation.
3) Students in school need awareness program on Cyber safety. This generation is techno savvy. If such programs conducted periodically, Cyber crimes in future can be minimized.

`

TESTING OF HYPOTHESES

As has been clearly indicated in the chapter of research methodology, testing of hypothesis has been offered in this chapter. Thus, an effort has been made to investigate, test and interpret the results of tests with detailed discussion on the methodology of the test procedure in the present section. In this view of matter present section has been divided into four sections and each section deals with the hypotheses, separately. Thus, Section-(a) tests hypothesis-H1 while Section-(b) tests hypothesis-H2 and accordingly Section-(c) and (d) bring out details on Hypothesis H3 and H4, respectively.

Testing of Hypothesis1

In this section detailed discussion has been offered for testing the hypothesis mentioned below. There Hypothesis 1 is expressed in two ways-Null (H_0) and Alternate (H_1)

> **H_1- There is a significant difference in the cyber safety awareness between age group of 18-30 years and above 30 years.**
>
> **H_0- There is no significant difference in the cyber safety awareness between age group of 18-30 years and above 30 years.**

For the purpose of testing hypothesis, technically, it has been presented in the form of hypothesis null and alternate with the help of **Table No. 64** below.

Table 64: Hypothesis-1

Sr. No.	Technical Hypotheses	Description	Mathematical Denotation
1	H_0– Hypothesis Null	There is NOT a significant difference in the cyber safety awareness between age group of 18-30 years and above 30 years.	H_0: Cyber Safety Awareness among age group of 18-30 years = Cyber Safety Awareness among age group of above 30 years
2	H_1 – Alternate hypothesis	There is a significant difference in the cyber safety awareness between age group of 18-30 years and above 30 years.	H_1: Cyber Safety Awareness among age group of 18-30 years ≠ Cyber Safety Awareness among age group of above 30 years

`

As it is well known, that awareness regarding any phenomena is the psychological term based on the knowledge possessed by the respondents regarding the term being investigated. Thus, during this investigation, an effort has been made to classify term cyber security considering certain needs of the end-users, such as, (a) Email account, (b) Social networking sites, (c) installation of antivirus software, (d) security of Wi-Fi network, (e) mobile phone security, (f) banking related cyber security, and (g) awareness regarding certain terms of cyber frauds. Considering all these needs, in present research awareness regarding cyber security has been measured as primary data which is collected through questionnaire-2. The basic tabulation regarding these parameters have been already discussed and presented in the chapter that follows.

Though, it has to be mentioned here that, all these parameters of the needs have been transformed into questions capturing required data set. Multiple methods of scaling and measurement have been adopted in the questions. It also needs to be highlighted that, there is no unique method of scaling and measurement found appropriate for measuring the data thus multifold technique of nominal and interval scales have been used while measuring awareness regarding cyber security from the respondents. All data measured and captured have been classified into two groups based on age factor as, (a) respondents belong to age category of 18 to 30 years and, (b) age category of 30 years and above. The next step adopted in testing procedure follows the summation of the responses collected through several questions. These arrived summations are used as measured level of awareness regarding cyber security and all the further statistical procedures are based on these calculated values.

Based on the **Table No. 64**, mean difference for ‘level of awareness regarding cyber security’ between ‘Age Group of 18 to 30’ and ‘Age Group of 30 and Above’ years has been accounted for 1.038 and the purpose of the hypothesis-H_1 is to test whether this difference between level of awareness is statistically significant or not. Considering all the details and based on the data ‘Independent Sample ‘t’ test found appropriate for the logical testing of this difference. These details of ‘t’ test have been mentioned below with the help of **Table No. 65**.

Table 65: Descriptive Statistics for Hypothesis 1

	Age (in years)	Mean	Std. Deviation	Std. Error Mean
Level awareness regarding cyber security	18 to 30	14.64	3.318	.101
	30 and Above	13.60	4.132	.291
Mean Difference		1.038		

Table 66: Calculation of 't' statistic for Hypothesis 1

Independent Samples Test									
	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
								Lower	Upper
Level awareness regarding cyber security (Equal variances assumed)	11.690	.001	3.908	1275	.000	1.038	.266	.517	1.560

`

On scrutinizing the results of calculations mentioned above in **Table No. 66** the inferences are as follows-

In case of hypothesis-H_1, one can observe that the Significance value obtained is less than 0.05. In such cases, the column labeled Sig. (2-tailed) displays a probability from the 't' distribution. The value listed is the probability of obtaining an absolute value greater than or equal to the observed 't' statistic, if the difference between mean of two groups is purely random. Since, confidence intervals lie entirely above 0.0; in this case, one can safely say that difference between observed level of awareness regarding cyber security of both age groups is statistically significant.

Hence, in this case, hypothesis null which states that "There is no significant difference in the cyber safety awareness between age group of 18-30 years and above 30 years" may be rejected and interpretation may be concluded as there is a significant difference between level of awareness regarding cyber security of age group of 18-30 years and the age group of 30 years and above by accepting alternate hypothesis.

Testing of Hypothesis 2

Hypothesis 2 is validated as follows:

H_1–There is association between various aspects of ICT which leads to the cyber crimes.

H_0–There is no association between various aspects of ICT which leads to the cyber crimes.

This hypothesis has involved two variables such as security policy using ICT and cybercrimes. Considering the various aspects of the present hypothesis, Q.2, Q.5, Q.17, Q.19, Q.21, Q.24 and Q.25 have been considered. The respondents have been asked that whether you receive emails or SMSs or Phone Calls that promise large sums of Money or Discounts (Q.21)? The answer for this question has been received in Yes or No type responses. An assumption for the answer 'Yes' involves further potential for cybercrime to happen. Then, it would be essential to check while analyzing this answers that whether these respondents are aware about implementing proper security practices while using ICT or not. For this assessment further questions have been asked to check awareness. The details of these questions have been mentioned below-

Table 67: Table based on Questions related to security practices

Question No.	Question	Assessment
Q.2	Is your password Strong? Does it contain following?	Awareness of using strong password
Q.5	Have you installed Antivirus Software on Your PC	Awareness of using antivirus
Q.17	Do you Note down Card and Customer Service no. on your mobile/card?	Awareness of running risk for potential cybercrimes
Q.19	Do you store your password, PIN, in your mobile as contact no.?	Awareness of running risk for potential cybercrimes
Q.21	Do you receive emails / SMSs / Phone Calls that promise large sums of Money/Discounts?	Entertaining the potential risks
Q.24	Have you uploaded following personal details on social networking sites?	Awareness of running risk for potential cybercrimes
Q.25	Do you accept unknown Friend's request?	Awareness of running risk for potential cybercrimes

Now, using question number 21 as a decision rule and splitting the data into two groups will fetch understanding regarding is there significant variation about those receiving big promising calls or SMS and whether those are aware about security practices of using ICT. Using Chi-square test separately for each variable of awareness and Q.21 will be appropriate to arrive at the conclusion regarding this hypothesis. Naturally, as used in ordinary Chi-square test, the technical hypothesis have been presented as below-

`

Table 68: Hypothesis 2

Sr. No.	Question No.	Question of Hypothesis	H_0	H_1
I	**II**	**III**	**IV**	**V**
1	Q-21 and Q-2, 5, 17, 19, 24, 25	Whether difference between observed frequencies and expected frequencies are significant?	there is no significant difference	There is a significant difference

Accordingly, required calculations of the chi-square test statistics based on expected frequencies and observed frequencies have been presented with the help of **Table 69** below.

Table 69: Chi-square Test Statistic for Hypothesis 2

Pearson Chi-Square	Value	df	Critical value for 0.05 Level of Significance
Q21 with Q2	715.28[a]	5	11.07
Q21 with Q5	18.97[a]	1	3.84
Q21 with Q17	1.09[a]	1	3.84
Q21 with Q19	2.62[a]	1	3.84
Q21 with Q24	32.64[a]	5	11.07
Q21 with Q25	92.69[a]	2	5.99
a)-0 cells (0.0%) have expected count less than 5. The minimum expected count is 6			

On scrutinizing the results mentioned in **Table 69**, interpretation is as below-

The chi-square test measures the discrepancy between the observed cell counts and expected cell counts. In the present hypothesis 0 cells (0.00 per cent) have expected frequency count less than 5, and minimum expected count is 6.00.

Thus, from the table above, it has been observed that the value of chi-square statistic in case of Q2, Q5, Q24 and Q25 is observed to be the tendency of larger magnitude than the value mentioned in the column 'Critical Value'. This leads to conclude that the variation between observed frequencies and expected frequencies are significant. Ultimately, it leads to rejecting null hypothesis. This means receiving emails / SMSs / Phone Calls that promise large sums of Money/Discounts have significant chances of rising cybercrimes in case of Q2, Q5, Q24 and Q25. Now in case of Q17 and Q19, value of chi-square statistic is observed to be the tendency of smaller magnitude than the value mentioned in the column 'Critical Value' leading to accepting null hypothesis. This means receiving emails / SMSs / Phone Calls that promise large sums of Money/Discounts have no association to the chances of rising cybercrimes in case of Q17, and Q19.

In an ultimate conclusion it may be pointed out that, receiving emails / SMSs / Phone Calls that promise large sums of Money/Discounts will be associated to chance of cybercrimes in case of practices such as, not having strong passwords, not installing antivirus on PC, uploading personal documents on social media sites and accepting unknown friend requests. While in case of noting down card and customer service number on mobile or card, and storing password, PIN in mobile as contact number isnot associated to cybercrimes in the context of receiving emails / SMSs / Phone Calls that promise large sums of Money/Discounts.

Testing of Hypothesis-H3

In this section, efforts have been made to generalize the observation regarding sufficiency of human resources in terms of dedicated manpower for cybercrime investigation. This aspect has been presented below in the form of hypothesis for the purpose of testing and further calculations.

> **H_1:** Cybercrime investigation has affected the Pune commissionerate due to the manpower available with the police stations for cybercrime investigation is inappropriate.
>
> **H_0:** Cybercrime investigation has not affected the Pune commissionerate due to the manpower available with the police stations for cybercrime Investigation is appropriate.

The hypothesis given above includes the variable of availability of manpower in proportion to the total manpower available at the commissionerate level. Simply, it means that nominal measurement has been adopted for the purpose of present hypothesis. Question No. 2 has been referred from the Questionnaire-4 for getting data collection from 13 police stations on Pune City in terms of Yes / No type answers for understanding the situation of adequacy of manpower available for cybercrimes investigations.

The simple frequencies obtained from the questions have been presented below with the help of **Table No. 70**.

Table 70: Simple Frequency regarding Status of adequate manpower availability

Questions	**Number of Police stations**		
	Yes	**No.**	**Total**
Dedicated manpower for cybercrime investigation	5	8	13

For the purpose of testing this hypothesis-H3 considering data mentioned in the table no. 7, it would be cleared that the method called hypothesis testing for proportions is the appropriate using 'z' statistic. As the assumption is indicated in the hypothesis that only 25 per cent of the police stations have dedicated manpower for the purpose of cybercrime investigation, technical hypotheses may be mentioned as below in **Table 71**.

Table 71: Hypothesis 3

Sr. No.	**Questions**	***Null Hypothesis***	***Alternate Hypothesis***
1	Dedicated manpower for cybercrime investigation	Not affected significantly	Affected significantly

Further calculations of hypothesis testing have been made with the help of below mentioned formula-$Z^1 = \frac{\hat{p}-p}{\sqrt{\frac{p.q}{n}}}$

`

Substituting the values in equations the results obtained have been presented below with the help of **Table 72.**

Table 72: Statistics for Hypothesis 3

Sr. No.	Variables	$\hat{p}$ (Observed value)	p (assumed value)	q	z	Signif-icance	z critical[2]
1	Adequate Manpower	0.3846	0.2500	0.7500	1.12	0.05	1.64

On securitizing the results mentioned in the Table 72 above, the inferences are as below-

For the variable 'availability of adequate manpower for investigation of cyber crimes', at 0.05 level of significance 'z' score obtained is as 1.12 and it is observed not to be greater than the critical value of standard normal distribution (arrived at 1.64) which comes under the acceptance region of hypothesis null. This leads to acceptance of alternate hypothesis H_1. With this situation, one can safely conclude that, **Cybercrime investigation has been affected the Pune commissionerate due to inadequate manpower for cybercrime investigation.**

Testing of Hypothesis 4

It has been assumed from the hypothesis below that; training provided to the staff will increase their efficiency of resolving cybercrimes during investigations. Based on this assumption below mentioned hypothesis has been formulated.

H_1: There is an association between training provided to staff and problems faced while investigation of cybercrimes.

H_0: There is no association between training provided to staff and problems faced while investigation of cybercrimes.

[2] Calculated online from the website: http://www.mathcracker.com/z_critical_values.php#results

`

In the present section this hypothesis has been tested and interpreted. In this view of matter, it has to be mentioned that, two variables are considered, namely, (a) Training provided to the staff and (b) problems faced during investigation of the cybercrimes. The data pertaining to these variables have been collected with the help of questionnaire-4 (to be specific, from question no. 3 and 10). Question-3 was asked to ensure whether the respondents have provided with sufficient training to investigate cybercrimes and Question-10 has been asked to capture whether these respondents face any problems during investigation. The respondents of these questions were officer of concerned police stations which highly underlines appropriateness of data and responses. The responses captured were in the form of Yes and No answers, showing nominal data. Thus assuming equal relationship between both the variables non-parametric Chi-square test found appropriate to test this hypothesis. Based on the discussion made above, technical hypotheses have been presented in below table.

Table 73: Technical hypothesis – H4

Sr. No.	**Question No.**	**Question of Hypothesis**	**H_0**	**H_1**
I	**II**	**III**	**IV**	**V**
1	Q-3 and Q-10	Whether difference between observed frequencies and expected frequencies are significant?	there is no significant difference	There is significant difference

Thus, accordingly, basic frequency tabulated has been provided below in **Table 74 *below***.

Table 74: Basic Frequency observed

Cross Tabulation of the Frequency obtained		Problems Faced during Investigation		
		Yes	No	Total
Training provided to the staff	Yes	1	8	9
	No.	4	1	5
	Total	5	9	14

With the help of SPSS-20, required statistical operations made on the data and chi-square statistic has been calculated. All these details have been presented in **Table 75 and 76** below.

Table 75: Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Training Provided * Problems Faced	14	100.0%	0	0.0%	14	100.0%

Table 76: Chi-Square Test Statistics

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.143[a]	1	0.285		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.					

On scrutinizing the results mentioned in **Table 76**, interpretation is as below-

The chi-square test measures the discrepancy between the observed cell counts and expected cell counts. In the present hypothesis 0 cells (0.00 per cent) have expected frequency count less than 5,and minimum expected count is 7.00.Thus, from the table above, it has been observed that the value of chi-square statistic is accounted for 1.143, which shows the tendency of larger magnitude than the value mentioned in the column 'Asymp. Sig. (2-sided)' that is 0.285. This leads to conclusion that the variation between observed frequencies and expected frequencies are significant. Ultimately, it may be safely concluded with rejecting null hypothesis that training provided to the staff has no significant association to the problems faced during investigation of cybercrimes.

`

Testing of Hypothesis 5

In the present section an effort has been made to investigate, test and interpret hypothesis based on the data collected from the police stations regarding cybercrimes registered and the number of cybercrime cases solved. Accordingly, the hypothesis has been presented as below-

> **H_1:** Cyber criminals are on rise since the number of crimes related to cyber security has not been resolved.
>
> **H_0:** Cyber criminals are not on rise since the number of crimes related to cyber security has not been resolved.

For the purpose of testing this hypothesis, total 34 police stations have been requested for providing data related to total cybercrime cases registered, solved and pending, though required data has been provided by 31 police stations for Year 2011 to 2016. For the purpose of testing hypothesis summation of year wise data has been made to arrive at total spectrum of cases during the entire period of 6 years. Table 83below provides the final data utilized for further calculation of hypothesis testing.

Table 77: Cybercrime cases registered and resolved during 2011-2016

Sr. No.	Police Station	Total Cybercrime cases registered during 2011-2016	Total Cybercrime cases resolved during 2011-2016	Percent of cases resolved during 2011-2016
1	**Yerawada**	19	4	21.05
2	**Vimantal**	11	4	36.36
3	**Vishrantwadi**	20	17	85.00
4	**Wanwadi**	22	11	50.00
5	**Kondhwa**	13	5	38.46
6	**Shivajinagar**	15	2	13.33
7	**Vishrambaug**	12	4	33.33
8	**Deccan**	51	28	54.90
9	**Kothrud**	31	11	35.48
10	**Bibvewadi**	1	1	100.00
11	**Swargate**	11	5	45.45
12	**Bund Garden**	39	6	15.38
13	**Koregaon Park**	12	7	58.33
14	**Lashkar**	92	56	60.87
15	**Chinchwad**	10	9	90.00
16	**Bhosari**	3	1	33.33
17	**MIDC Bhosari**	4	4	100.00
18	**Sangavi**	7	1	14.29
19	**Cyber Cell**	271	102	37.64
20	**Khadki**	9	0	0.00
21	**Mundhwa**	1	0	0.00
22	**Sahkarnagar**	5	0	0.00
23	**Marketyard**	1	0	0.00
	TOTAL	660	278	
	MEAN	**40.14**		
1	**Hadapsar**	0	0	0.00
2	**Faraskhana**	0	0	0.00
3	**Samarth**	0	0	0.00
4	**Wakad**	0	0	0.00
5	**Hinjewadi**	0	0	0.00
6	**Pimpri**	0	0	0.00

From the table above, it can be noted that, out of 31 police stations, 6 have reported ‘zero’ (no) cybercrimes in their area. Thus, these ‘no cybercrime’ police stations have been excluded from further procedure of hypothesis calculation.

For testing of Hypothesis 5, arithmetic mean of the cases resolved has been worked out and recorded in the Table 83, as 40.14. In the hypothesis 30.00 %

cases resolved would be considered as significance to rise of cybercriminals. And the observed mean of cases resolved is 40.14 per cent. In this section efforts have been made to test the significance of difference (10.14) between assumed mean of cases resolved (that is 30.00) and observed mean (that is 40.14). This situation lead to applying 't' test for testing this hypothesis and technical hypotheses have been presented below in **Table 78**.

Table 78: Testing of Hypothesis 5

Sr. No.	**Question of Hypothesis**	**H_0**	**H_1**
I	**III**	**IV**	**V**
1	Criminal on rise and number of cases resolved	there is no significant difference	There is a significant difference

The required calculations for 't' statistic has been computed using SPSS-20 version and have been presented below in Table 79 and 80.

Table 79: One Sample 't' Statistics for Hypothesis 5

	N	Mean	Std. Deviation	Std. Error Mean
Percent of Cases Resolved by police stations	23	40.14	31.41	6.55

Table 80: One-Sample Test

One-Sample Test						
	Test Value = 30.00					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the difference	
					Lower	Upper
Percent of Cases Resolved by police stations	1.548	22	.136	10.13913	-3.4470	23.7253

On scrutinizing the results of calculations in Table 79 and 80, in the case of hypothesis 5, one can conclude that because the Significance value obtained shows a tendency to be greater than 0.05; in such a case, the column labeled Sig. (2-tailed) displays a probability from the t distribution with 22 degrees of freedom. The value listed is the probability of obtaining an absolute value greater than or equal to the observed *'t'* statistic, if the difference between the sample mean and the test value is purely random. Since, confidence intervals lie slightly below 0.0; in case of Hypothesis 5, one can safely say that observed percent of resolving cases is not significantly different from assumed mean of 30. Hence, it may be inferred that alternate hypothesis can be accepted i.e., **"Cyber criminals are on rise since the number of crimes related to cyber security has not been resolved."**

CHAPTER 5 –CONCLUSIONS & RECOMMENDATIONS

This chapter is discussed under the following headings:

5.1 – Introduction

5.2 -- Cyber crimes in Pune city

5.3 – Objectives of present study

5.4 - Conclusions

5.5– Recommendations to

1) Government of India
2) Government of Maharashtra
3) Organizations
4) Education Sector
5) Cyber Cell / Police stations
6) Cyber Forensic Lab
7) Internet Service Providers

5.6 – Areas of further research

5.1 Introduction

This research was focused on study of various factors affecting effective investigation of cyber crimes in Pune city.

Researcher first studied cyber crimes status of various states of India where there are highest number of cyber crimes. Then Researcher focused on Maharashtra because cyber crimes in Maharashtra state in last 5 years are rising und are highest as compared to other states. It was found that Pune city has the highest number of cyber crimes compared to other cities in Maharashtra.

The researcher's place of Residence is also Pune therefore Pune city was selected for further research. Researcher selected all 39 police stations from Pune city and PCMC area to get information on cyber crimes such as Cyber crimes registered, investigated and pending in last 5 years, the problems faced by cyber crime investigation officers and ACPs, DCPs of those police stations.

Before starting the actual research, Researcher studied the best practices of other countries related to cyber security. "Organizational Structure" of Maharashtra Government is reviewed before starting the collection of information.

This has made the clear view of cyber crime status in India and abroad, cyber security best practices of other countries etc..

Various Journals, policies, security reports of competent organizations were studied. Books of experts, daily news papers gave insight of cyber crimes scenario at present in India and other countries.

.Various ACPs, DCPs, as well as cyber crime investigation officers along with Research Guide helped time to time to give insight about the research work.

Literature Review for this Research carried out in a systematic manner such as Survey of International reports, survey of reports in India, related research papers, articles on cyber crimes, cyber security, cyber attacks, legal aspects etc. Literature review has helped to get insight of the topic as well as the gaps which has helped for further research.

5.2 Cyber Crimes Scenario In Pune City

Cyber crimes in various cities of India were studied initially. After the study, **Maharashtra** was selected to study cyber crime scenario. From this, **Pune** was selected as there are rising cyber crimes compared to other major cities of Maharashtra like Mumbai, Nagpur, Nasik, Aurangabad.

Statistics of Cyber crimes registered, investigated and pending from all 39 Police stations of Pune city and PCMC area of last 5 years (2011-2016) were collected under RTI. This study has revealed that there is inverse proportion of cyber crimes registered and investigated. Therefore there is great number of pending cyber crimes. As this gives rise to space for cyber criminals to commit more number of cyber crimes, this research has been under taken.

From the present study, it has been revealed that cyber safety awareness amongst age group of 18-30 years and above 30 years is low. This resulted in committing more cyber crimes.

Disposal rate of Cyber crime cases in last 5 years (2011-2016) is not very optimistic in Pune city because of various reasons. The cyber crimes in last 5 years are increasing.

The cyber cell and cyber forensic lab of Pune facing many problems due to lack of dedicated manpower, technology and devices required for search and seizure of cyber crimes and relevant training required for handling particular type of cyber crime case investigation..

To understand the problem while investigating cyber crimes, various respondents were communicated via personal visit and through Questionnaire under RTI. Cyber Crime investigation officers, Assistant Commissioner of Police (ACP), Deputy Commissioner of Police (DCP), Cyber crime Investigation Consultants, Cyber Lawyers, Investigation officers of Cyber Forensic lab were interviewed for this research.

To understand the Cyber Safety Awareness amongst the Internet users,1122 respondents were selected for the study.

According to National Crime Records Bureau (NCRB) of India, Cyber crimes between age group of 18-30 years are significant compared to age group 30 years and above. Therefore 49, 352 school children between age group of 11-16 (Std V to X) were selected to make them acquainted with Cyber Crimes and Cyber Safety. They were given presentations. Feedback of School Principals / Coordinators was obtained which highlights the need to make these techno savvy children aware on 'Cyber Safety'.

5.3 Objectives of Present study

The proposed study attempted to address many aspects of rising cyber crimes and problems occurring while cyber crime investigation.

The main objectives of the study, therefore, were

1) To find out 'Cyber safety Awareness' amongst age group of 18-30 years and above 30 years.
2) To find out the crimes registered and crimes investigated in all Police stations of Pune city where Cyber cells are there.
3) To find out factors affecting effective investigation of cyber crimes in Pune region from experts in this area.
4) To impart training to school children of age below 18 years so that they will be more aware on cyber crimes.
5) To propose a new model for cyber crime investigation process that will help all Cyber cells, Cyber Forensic lab and Police stations of Maharashtra for timely investigation of cyber crimes.

5.4– Conclusions

The conclusions of the entire research have been discussed in the light of the objectives.

1.The first Objective of the study was **To find out 'Cyber safety Awareness' amongst age group of 18-30 years and above 30 years.**

The data on '**Cyber Safety Awareness'** from people of age group of 18-30 years and above 30 years was collected and valid data of 1122 was considered for research study.

The data on **"Cyber Safety Awareness"** collected based on certain questions related to (a) Email account, (b) Social networking sites, (c) Installation of antivirus software, (d) Security of Wi-Fi network, (e) Security of mobile phone, (f) Cyber security related to banking, and (g) awareness regarding certain terms of cyber frauds

From the results of present study it was found that there is significant difference related to "Cyber Safety Awareness" between both the age groups. There is need to conduct **"Cyber Safety Awareness Campaign"** for different age groups so as to minimize the rising cyber crimes.

2. The second Objective was **To find out the cyber crimes registered and Crimes investigated in all Police stations of Pune city.**

The data of cyber crimes U/s 65, 66(A-E) , 67 from the year 2011-2016 of all 39 police stations from Pune city was collected through personal visit and Questionnaire. The reason to select the data from theses sections only is that the cyber crimes reported are high compared to other sections. Out of 39 Police stations, 34 police stations i.e. 87% out of 39 responded to it. This has increased the validity of proposed research.

It was found that there is inverse proportion of cyber crimes registered and cyber crimes investigated. This study showed that percentage of pending cases is very high. This has also highlighted that cyber crime investigation process is not effective.

3.The third Objective was **To find out factors affecting effective investigation of cyber crimes in Pune region from experts in this area.**

Based on Conclusion 2, the survey of 10 police stations coming under 6 main Divisions of Pune city and PCMC area was done. The questionnaire related to "Problems faced by cyber crime investigation officers" was given.

This questionnaire was well responded by all Divisions of Pune city and PCMC area. Various questions related to Man power, Training to Police officers for cyber crime investigation, CDR (Call Detail Record), response from ISP (Internet Service Provider), type of frauds, Support of external agency or technical person to resolve cyber crime, legal issues, support of foreign countries on cyber crime investigation were asked to ACPs or DCPs.

From the data obtained it can be concluded that Police stations need dedicated trained man power, latest hardware and software technology and devices for cyber crime investigation, quick response from Internet Service Providers and cooperation of foreign countries during investigation of social networking crimes.

4**.**The fourth Objective was **To impart training to school children of age below 18 years so that they will be more aware about cyber safety and cyber crimes.**

After literature review, it came to know that cyber crimes committed by the age group of 18-30 years are more. Also from the survey of 1122respondents it was found that the ‘Cyber Safety Awareness’ amongst internet users is very less which may result in falling victim to cyber crimes. This has highlighted the need to train school children below 18 years.

In this context, 49,352 students from 76 different schools in Pune and PCMC area were sensitized for cyber safety awareness. These children were sensitized by a group of College students who were trained on **Cyber Safety** by few Colleges in Pune city.

After this cyber safety awareness program, the need to impart training on ‘Cyber Safety Awareness’ from all school Principals / Coordinators of Pune city and PCMC area was highlighted. They suggested to frequently organizes such lectures for School children and make them aware about Do’s and Don’ts while using smart devices / technologies (mobiles, computers, laptops or other gazettes etc) , during online chats, online shopping or while using social networking sites.

5. The fifth Objective was **To propose a new model for cyber crime investigation process that will help all Cyber Cells, Cyber Forensic lab and Police stations of Maharashtra for timely Investigation of cyber crimes. [Please refer to Figure]**

Table 81: Existing System & Problems Vs Proposed System & Solutions

Sr. No.	Existing System and Problems	Proposed System and Solutions
1.	Existing System of FIR registrations is in offline mode (i.e. complaint is registered in person in police stations). FIR format is available online but accepted in person.	Instead of Format, online form should be filled by Complainant or Police stations should fill the form online in police station from complainant which will include Personal details of Complainant and type of cyber crime or other required details. These details can be available any time if recorded in online mode.
2.	Case Investigation Details	
a.	**IRT reports**- The report of cyber crimes collected using IRT (Incidence Response Toolkit) is recorded offline.	If this report will be entered in computerized format through ERP system by cyber forensic lab and transferred online to police stations or can be made online available for review using authentic password, ill further save time of investigation.
b.	**Forensic Details:**	Other Forensic details or observations noted by cyber forensic departments are sent to Police stations or cyber cells directly or can be made online available for review using authentic password. This will help accelerating cyber crime investigation process.
c.	**ISP details**	If Internet Service Providers send the details in time, it will help cyber cells and cyber lawyers to quickly investigate the case. These details can be recorded as ERP system to relate it with other required data of crime investigation to quickly review the facts.
d.	**Judiciary Process** Judiciary Process depend on all evidences generated from primary investigation, ISP reports, IRT reports etc.. If any of the reportis not furnished properly or in time, it will delay judgment procedure.	Decisions of Judges or cyber lawyers will become easy if reports of cyber forensic lab, ISP and IRT received in time. Final judgment will help to resolve the cyber crime cases and cyber criminals will not get space to commit more cyber crimes in future.
e.	Case Investigation details are given to Investigation Officer by different people at different times. If any record is missing or not getting in time, it will impact cyber crime investigation process.	If case investigation details are available online, Investigation Officer can get all the details at a glance such as Forensic reports, primary reports from cyber cell, ISPs reports. cyber lawyer's reports etc. This will help to resolve cyber crimes at a faster rate.
f.	Transfer of ACP / DCP or change of CIO (Crime Investigation Officer) delays cybercrime investigation process.	ERP System integrated with all the modules will help any new investigation status and proceed further. This will not delay the crime Investigation Process**.**

Proposed Model For Accelerating Effective Cyber Crime Investigation Process

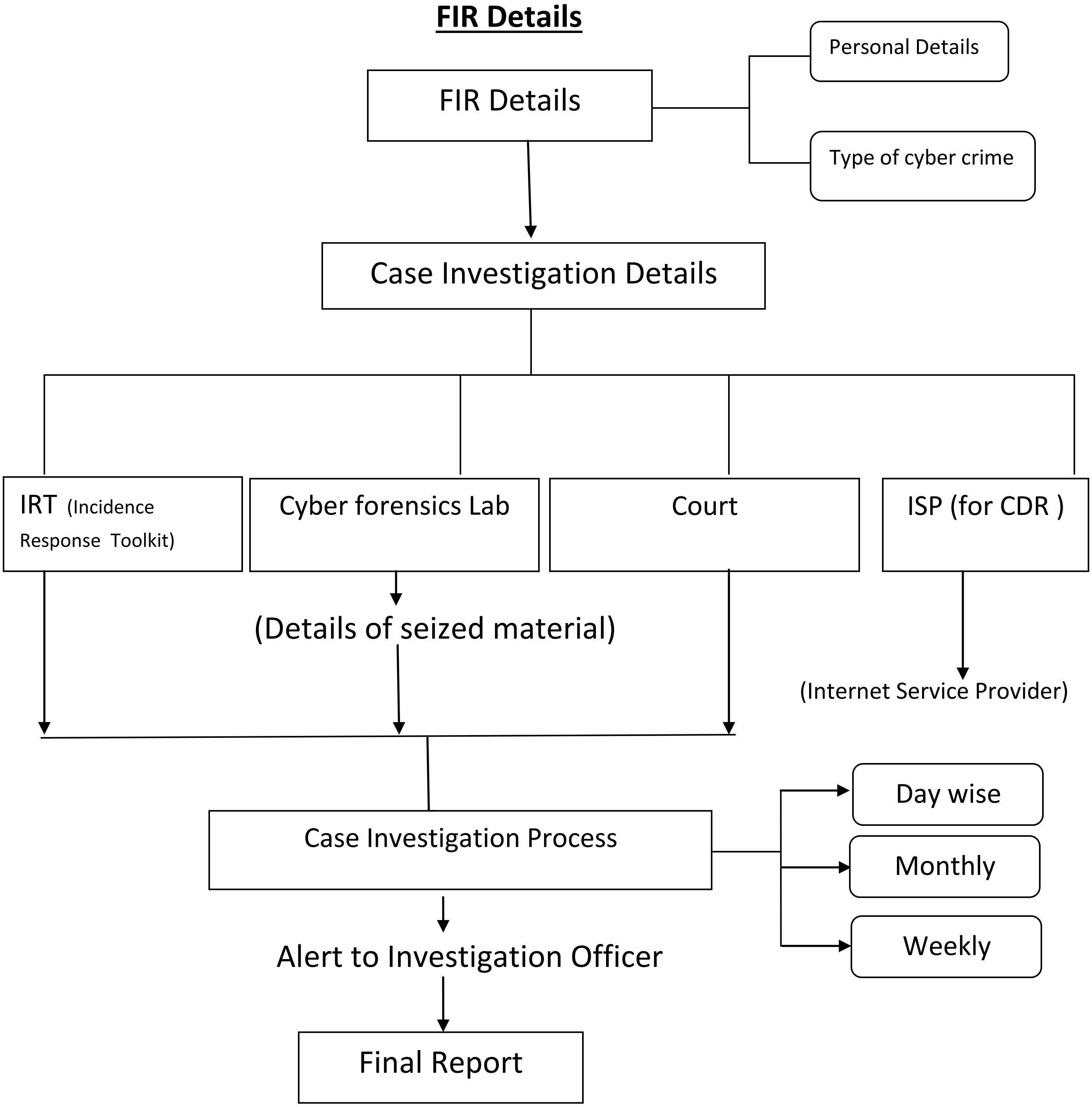

FIR Details
FIR Details
Personal Details
Type of cyber crime
Case Investigation Details
IRT (Incidence Response Toolkit)
Cyber forensics Lab
Court
ISP (for CDR)
(Details of seized material)
(Internet Service Provider)
Case Investigation Process
Day wise
Monthly
Weekly
Alert to Investigation Officer
Final Report

Figure 31: Proposed Model of "Computerized Cyber Crime Investigation System" for effective investigation of cyber crimes in India

<u>Proposed ERP model for investigation of cyber crimes in India</u>

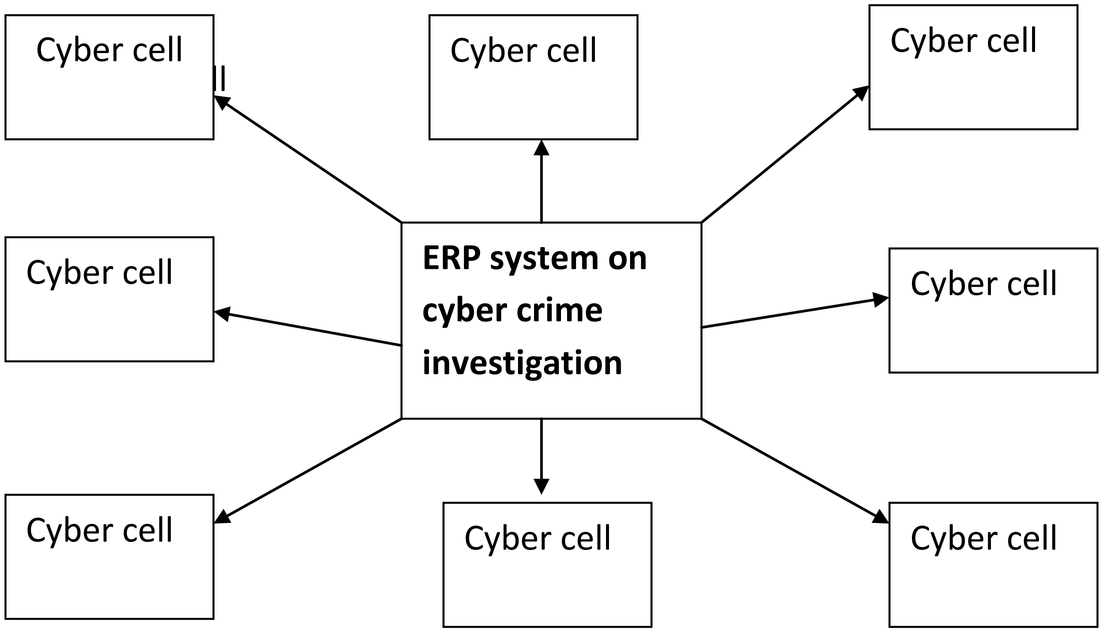


Figure 32: Proposed ERP model

5.5- Recommendations

After a detailed research and understanding of the cyber crime scenario and modus operandi for cyber crime investigation, the researcher would like to recommend the following to:

1) **Government of India**

   a) A mass program for ‘Cyber Safety Awareness’ should be carried out by Government of India Under ‘National Skill Development Council (NSDC)’ of India.

   b) Government of India should make it compulsory for Foreign Companies to obey the laws and rules of India when they are doing their business in India.
   e.g. Servers of Social networking sites are located outside India or in foreign countries and obeys the laws of host countries. When cyber crime happens and victim is affected in India which has origin in foreign country, Cyber crime Investigation officers are not getting timely help or required information from companies based in foreign countries.

   c) Government should take initiative for developing MLTs (Mutual Law Treaties) between two countries for solving Legal problems while investigating cyber crimes.

   d) Creating our own Servers for internet, social networking sites and online shopping.

   e) Making it compulsory to use biometric while withdrawing money from Bank ATMs to avoid ATM frauds.

   f) “Cyber Crime Helpline or Toll free number” must be given by Police stations to help people. This will give quick help of Police officers.

   g) Government should warn banks, ISPs to co-operate timely to give timely information for investigation of cyber crimes.

   h) Government must conduct Cyber Safety Survey of Cities especially metro cities or cities declared as smart.

i) There is need to study cyber crime investigation strategies and procedures of cyber crime investigation of different countries which are top in cyber security. There is need to know global measures to curb cyber crimes.

j) There is no proper hands on training to Police department how to handle digital evidences or practical training of investigating particular crime such as hacking, phishing etc.

k) There is need of study of acceptability, reliability and authenticity of e-records. There must be guidance from experts on 'Best evidences Policy' while doing cyber forensics investigation.

l) Technical experts should be appointed in cyber cells for investigation of cyber crimes. There is need to involve Engineers or technical experts for investigation of cyber crimes in IP detection, search and seizure operations, Data recovery, Hard disk protection, code protection after cyber crime committed at site, giving proper digital evidence in the court, handling latest softwares for cyber crime investigation etc..

2) Government of Maharashtra

a) Maharashtra Government should establish a separate state-of the-art 'Cyber Crime Investigation Cell' which will handle only cyber crimes in Pune city and PCMC area. This Cell will feature following:

- ➢ Online FIR
- ➢ Trained and adequate manpower
- ➢ Latest Hardware and Software for Cyber crime investigation
- ➢ Practical Training to people involved in investigation for handling digital evidence.
- ➢ Training for search and seizure operations of cyber crimes
- ➢ Well equipped Cyber Forensic lab

b) There should be software for speedy investigation of cyber crimes that stores status of crime investigation such as cyber crimes registered, investigated, pending, persons arrested, sections of IT/IPC Act applied, name of person handling case, cyber crime investigation officer etc..

c) Smart cities should be made cyber secure first by conducting training of people of all age groups from different sectors on cyber safety awareness.

d) Training to police officers should be given for identifying type of cyber crime and register it under particular section of IT Act /IPC Act /or both.

e) Need to create 'Cyber Safety Awareness' amongst different age groups of Pune city such as Working professionals, House wives, senior citizens etc..

- The age group of 18-30 years needs special attention as ***cyber crimes committed*** as as well as ***persons arrested*** in this age group are more compared to other age groups.
- "Cyber Safety training program" needs to be created for school children below 18 years as this generation is more techno savvy.
- Special training should be given to people above 30 years by Police department.

3) Organizations

a) Every organization should make its 'Information and Cyber Security Policy'.

b) CII (Confederation of Indian Industries), NASSCOM (National Association of Software Companies), CSI (Computer Society of India), DSCI (Data Security Council of India) must undertake cyber safety awareness campaign for rural areas.

4) Education Sector

a) Every Educational Institute should make its 'Information and Cyber Security Policy'.

b) Schools and colleges need to form 'Cyber Awareness Literacy Cell' to spread awareness on cyber safety in school children of age group 11-16 years and in Junior and Senior colleges above 16 years.

5) **Cyber Cell / Police stations**

   a) The cyber crimes should be reported and accepted online through online FIR system.

   b) The training of IT Act and registering cyber crimes under various sections of IT Act be given to all police officers.

6) **Cyber Forensic Lab**

   Cyber Forensic Lab during cyber crime investigation, need to use latest technology for search and seizure operation of digital evidence such as updated hardware's and softwares.

7) **Internet Service Providers (ISPs)**

   a) Making it compulsory to all Internet Service Providers for giving timely CDR (Call Detail Record) in case of mobile or internet related crimes.

8) **Internet Users**

   a) Windows O.S. can be replaced with Open source :

Windows Operating System needs antivirus software. Though Windows 10 is fee recently, old versions were costly. For Windows O.S., antivirus softwares are required and have cost. Considering the benefits of Open Source Softwares which are freely available, motivation to use these softwares should be done. Linux O.S. is free. It does not require to install antivirus software like Windows. Windows O.S. based Softwares are costly whereas Linux O.S. based softwares are free. Besides this, other features that motivates to use open source softwares are

- Ease of use
- Reliability
- Highly Secure O.S.
- Massive online support for problems
- Widely used by various organisations such as corporates, Scientists, Educational Institutes, IITs and NASA.

b) Securing from Public Wi-Fi Threats:

By using aVirtual Private Network (VPN) ,users can keep their information safe from public Wi-Fi threats. VPN creates a safe and encrypted connection over a less secure network, such as the internet.

c) There is need to add additional security layer to products such as

a) Use of strong passwords while using online mode of transaction.

b) Use of Firewall along with Antivirus.

5.6 Areas of further research

1) The present research is carried out in Pune region but is must for every city in Maharashtra and also other states of India.
2) Cyber forensic investigation area can be given due importance for study as it plays important role in cyber crime investigation.
3) Study of Policies of countries having ‘Zero or minimum cyber crimes’ can be undertaken.
4) Yearly Cyber safety Literacy survey of every city can be done in India.
5) Model proposed for effective cyber crime investigation can be developed further and implemented. This will increase rate of cyber crime investigation process. This will help to catch and punish cyber attackers in time. This will create fear in future cyber attackers who wish to commit cyber crimes.
6) ERP Software for effective cyber crime investigation process can be developed further that will save time for manual work related to cyber crimes and will link all Cyber Cells in the Country.
7) Research on ‘Cyber Safety and Security Policies’ of different organizations can be done.

CHAPTER 6 – REFERENCES

A. S. (2013, November 21). The Social Networth. *Times Of India*, p. 4.

Agarwal, S. C. (February - 2001). Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements. *CBI Bulletin,* 4-11.

Ali, M. M. (June 2016). Determinants of preventing cyber crime : A survey research [Abstract]. *International Journal of Management Science and Business Administration,2*(7), 16-24. doi:10.18775/ijmsba.1849-5664-5419.2014.27.1002

Ansari, M. (2016, October 25). Member of Auto rickshaw gang that looted over so many people in a year nabbed. *Pune Mirror*.

Behra, A. (2010). Cyber crime and Law in India. *Indian Journal of Criminology and Criminalities,* 16-30.

Brown, C. S. (2015). Investigating and Prosecuting Cyber crime: Forensic dependencies and barriers to justice [Abstract]. *International Journal of Cyber Criminology,9*(1), 55-119. Retrieved October 18, 2017.

Cheating via online business. (2016, September 23). *Sakal*.

Chaubey, R. K. (2009). *An Introduction to cyber Crime and Cyber Law* . Kamal Law House Publication.

CM under pressure- to`sack under cops. (2012, November 21). *Times Of India*, p. 1.

Computer Games. (February 2011). *CSI Communications, 34*(11), ISSN 0970-647 x, 16-18.

Crime Statistics 2011.Retrieved April 25, 2014, from http://www.ncrb.org

Crime Statistics 2012.Retrieved May 10, 2014, from http://www.ncrb.org

Crime Statistics 2013. Retrieved January 11, 2015, from http://www.ncrb.org

Crime Statistics 2014. Retrieved August 31, 2015, from http://www.ncrb.org

Crime Statistics 2015. Retrieved September 23, 2016, from http://www.ncrb.org

Crime Statistics 2016. Retrieved October 2, 2017, from http://www.ncrb.org

Cyber Security Task Force. Retrieved May 25, 2015, from https://www.dsci.in/sites/default/files/Coverage%20of%20DSCI-Lockheed%20DSCI%20launch%20cyber%20educational%20portal.pdf

Cyber Crimes. Retrieved July 20, 2015, from http://cybercellmumbai.gov.in

Cyber Threats. (2012, November 21). *Times Of India*, p. 4.

Dalal, A. S. (2010). Jurisdiction in cyber space .*M.D.U. Law Journal,* 37-56.

Dasgupta, M. (2009). *Cyber Crime in India: A Comparative Study*. Eastern Law House Publication.

Dudeja, V. D. (2002). *Cyber Crime and the Law*. Commonwealth Publication.

E-Company cheated for 11 crores. (2016, September 23). *Maharashtra Times*

Gang arrested by cyber cell, Pune in Credit card frauds. (2016, October 4). *Maharashtra Times, Pune ed.*.

Girls Swear of Social Media . (2012, November 21). *Times Of India*, p. 10.

GIS. (February 2012). *CSI Communications, 35*(11), ISSN 0970-647 x, 35-37.

GIS. (January 2012). *CSI Communications, 35*(10), ISSN 0970-647 x, 30,32.

Green Computing. (January 2011). *CSI Communications,34*(10), ISSN 0970-647 x, 30.

Indian Security Products -Countering Cyber Risks . Retrieved April 18, 2016, from http://www.nasscom.in/custom_search/node/cyber%20security

Growing Cyber Security Industry-Roadmap for India. Retrieved July 20, 2016, from https://www.dsci.in/content/studies-reports

Investigation of cyber crime in Police station. (2016, November 30). *Sakal*.

Kadam, A. (2012). Information Security- Personnel Security-|Defense in Depth. *Data Compression, 35*(12), ISSN 0970-647x, 30-31.

Kadam, A. (2012). Network Security-Defense in Depth. *Geographic India System,* *35*(10), ISSN 0970-647x, 30-31.

Kadam, A. (2012). Physical Security -Defense in Depth. *Geographic Information System (GIS), 35*(11), ISSN 0970-647x, 36.

Kamath, N. (2009). *Law Relating to Computers, Internet and E-commerce: A guide to Cyber Laws and the Information Technology Act, 2000.* Universal Law Publishing Co.

Kothari, C. R., &Garg, G. (2014). *Research Methodology-Methods & Techniques* (3rd ed., Vol. 3, ISBN:978-81-224-3623-5). New Delhi, Maharashtra: New Age International (P) Ltd.

Karwan, K. M. (June-2015). An Investigation into cyber security in terms of costs, impacts and occurrence of current ICT issues in front of private sectors and electronics governments. *International Journal of Scientific and Engineering Research ,6*(6), 970 ISSN 2229-5518.

Kotwal, S., & Manhas, J., Dr. (2017). Investigation of different constraints in cyber crime and digital forensics [Abstract]. *International Journal of Advanced Research in Computer Science and Software Engineering,7*(7), 2277-128, 222-227. doi:10.23956/ijarcsse/v7170209

Kumar, S., Koley, S., & Kumar, U. (april-2015). Present Scenario of Cyber crime in India and its preventions. *International Journal of Scientific and Engineering Research, 6*(4), 1971 ISSN 2229-5518.

Loader, B., & Thomas, D. (2000). *Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge Publication.

Lutta, V. O., & Obiril, J. F. (march-2015). Cyber Crime -a Rising Threat for Internet-Based Businesses in Western Region, Kenya.*International Journal of Scientific and Engineering Research, 6*(3), 371 ISSN 2229-5518.

Mali, P. (2012). IT Act 2000- Software Piracy & Indian Law. *Geographic Information System (GIS), 35*(10), ISSN 0970-647x, 32-33.

Marcellai JA, & Greenfield, R. S. (2002). Cyber Forensics-A Field Manual for Collecting, Examining and Processing Evidence of Computer Crimes.

Marcellai JA (November 7). How to Prime your new personal Computer. Times Of India, Pune ed., p. 3.

Mali, P. (2012). Data Loss Prevention (DLP). *Geographic Information System (GIS), 35*(11), ISSN 0970-647x, 35.

Mali, P. (2013). *Cyber Law and cyber Crimes* (1st ed., Vol. 1, ISBN:978-81-8159-574-4). Mumbai, Maharashtra: Snow White.

Mali, P. (2013). *Cyber Law and cyber Crimes*(1st ed., Vol. 1, ISBN:978-81-8159-574-4). Mumbai, Maharashtra: Snow White .

Man Nabbed for dupling over 500 people via fake company. (2013, September 23). *Pudhari*

Muddaraju, N., & R. (August - 2009). Cyber Crimes: Need an Effective Law. *Criminal Law Journal* , 227-231.

Nagpal, R. (July 2002). Offences and penalties under the Information Technology Act, 2000. *Information Technology Law Journal* , 15-32.

Nagpal, R. Evolution of Cyber Crimes . Retrieved May 25, 2015, from http://www.cyberlawdb.com/docs/ebooks/cc.pdf

Online Safety Tips. Retrieved June 10, 2016, from http://www.punepolice.gov.in/content/cyber-crime-cell-awareness-notes

Paranjape, V. (2010). *Legal Dimensions of Cyber crime and Preventive Laws-with special reference to India* (1st ed., Vol. 1). Allahabad, Uttar Pradesh: Central .

Parthsarthi, P. (2012). Cyber Crimes. Retrieved January 15, 2016,

from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

People arrested for looting people through credit card. (2016, October 4). *Pudhari*.

Ryder, R. D. (2001). *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet)*. Wadhwa Publication.

R. (2009). Pornography and Obscenity on the Web: Need a strict Law. *Supreme Court Journal,* 20-25.

Positioning India as a Cyber Security Hub. (2016, January 7). Retrieved Jan 9,2016,from http://www.nasscom.in/sites/default/files/NASSCOM_Annual_Report_2015-16.pdf

Safety Tips. Retrieved June 15, 2015, from http://www.punepolice.gov.in/content/safety-tips-and-preventions

Sharma, R. (2012). Study of latest Emerging Trends on cyber Security and its challenges to Society. *International Journal of Scientific and Engineering Research, 3*(6), 1 ISSN 2229-5518.

Sharma, V. (2010). *Information Technology: Law and Practice*. Universal Law Publication Co.

Sharma, A. (Sept.2017). Globalization and its impact on cyber crime : case study of Indian Police Administration. *Docplayer,* 1-17. Retrieved September 27, 2017.

Sharma, S. C., Dr. (2008). Study of Techno-Legal Aspects of Cyber Crime and Cyber Law Legislations. *Nyaya Deep,* 86.

Singh, Y., Justice. (2007). *Cyber Laws*. Universal Law Publishing Co. Pvt. Ltd.

Sood, V. (2010). *Cyber Crime, Electronic Evidence & Investigation Legal Issues* (1st ed., Vol. 1, ISBN-978-81-7274-707-7). New Delhi, Uttar Pradesh : Nabhi Publication.

Various Cyber crimes. Retrieved November 7, 2016, from http://cybercellmumbai.gov.in/html/cyber-crimes/index.htm

Verma, S. K., & Mittal, R. (2004). *Legal Dimensions of Cyber Space* . Indian Law Institute Publication.

Vyas, S., & Vyas, K. K. (September-2015). Virtual Parliament-An immediate need of digitally Ready India. *International Journal of Scientific and Engineering Research, 6*(9), ISSN 2229-5518.

Yadav, S., T., & Arora, Y. (2013). Cyber crime and Security. *IJSER International Journal of Scientific and Engineering Research,4*(8), 856 ISSN 2229-5518.

QUESTIONNAIRE-1

Information of Cyber Crime cases (Year 2009-2012) from various Cyber Cells and Cyber Forensic Lab of Maharashtra under RTI Act (Right to Information Act)

Types of Frequent Cyber crimes	**No. of Crimes Reported /Registered**	**No. of Cyber Crimes Resolved**	**No. of Crimes under Investigation**	**Pending cases with reason**
Email Threat				
Data Theft				
Website Hacking				
Phishing				
Credit card Fraud				

Questionnaire-2

CYBER SECURITY LITERACY PROGRAMME

Cyber Safety Awareness Survey in Pune City

[Digital India Week-7th July 2015]

Personal Information :

1) Name : - ____

2) Mobile No. :- ______________________________

3) Gender :- M / F 4) Qualification: -

5) Age Group : - a) 18-30 yrs. b) 30-45 yrs.c) 45- 60 yrs.d) Above60yrs.

Quiz on Cyber Security

1) Do you have an email account? :- a) Yes b) No

2) Is your password strong? Does it contain following-

a) Alphabet b) Number c) special characters d) alpha numeric

e) Combination of all

3) Do you change password frequently? :- a) Yes b) No

4) Which Social Networking sites you use?

a) Facebook b) Twitter c) Whatsapp d)Any other

5) Have you Installed Antivirus Software on Your PC? :- a) Yes b) No

6) If Yes which software?

a) McAfee b) E-scan c) Quick Heal d) Symantec e) Any other

7) Have you purchased licensed software for your PC? :-

a) Yes b) No c) Not applicable d) Using Pirated Software

8) Have you installed Antivirus and Firewall on your PC?

a) Installed Antivirus only b) InstalledFirewall only

C) Installed both- Antivirus& firewall d)installednone

9) Do you have different passwords for email and Social media accounts?

a) Yes b) No

10) Is your Internet Wi-Fi password secure? a) Yes b) No

11) Do you take Backup of sensitive and important information? a) Yes b) No

12) Do you use UPS for Backup? a) Yes b) No

13) Do you know IMEI of your mobile phone? a) Yes b) No

14) Which card you use for financial transaction?

a) Debit Card b) Credit Card c) Both d) None

15) Do you proper "log out "after using email account, Internet banking Services?

a) Yes b) No c) I just Close Window

16) Do you store you password, Pin in your Mobile as Contact No?

a) Yes b) No

17) Is your Bluetooth on? a) Yes b) No

18) Do you receive emails/SMSs/Phone calls that promise large sum of Money/Discounts? a) Yes b) No

19) If yes, then do you respond? a) Yes b) No

20) If yes, then how you respond?

a) By replying to SMS/email

b) By calling contact no. given in email/SMS

c) By entertaining their call

21) Have you uploaded following personal details on social Networking Sites?

a) Your Photo b) contact no. c) Email d) Address e) All

22) Do you accept unknown friend's request?

a) Yes b) No c) Sometimes

23) Have you heard about following terms?

a) Nigerian Fraud b) Credit Card Fraud c) Phishing

d) Identity Theft e) Hacking f) All above

Cyber Crime Investigation Status in Various Police Stations in Pune city (2011-2016)

Types of Cyber Crimes & under Section No.	No. of Crimes Reported / Registered	No. of Crimes Resolved	No. of Crimes under Investigation	Pending Cases with reasons
Offences under IT Act				
Tampering computer source documents (Sec.65)				
Computer related offences (Sec.66 and Sec.66 A to E)				
Under Section 66 and 66A				
Under Section 66B				
Under Section 66C				
Under Section 66D				
Under Section 66E				
Cyber Terrorism (Section 66F)				
Publication/transmission of obscene / sexually explicit act, etc. in electronic form (Sec.67 and Sec.67 A to C)				
Offences under IPC Act (involving Computer as Medium/Target)				
Cheating (Section 420)				
Credit / Debit Card				
Others				

QUESTIONNAIRE- 4

Study of Problems faced by Police stations in Pune city during investigation of Cyber Crimes

1	Is there any special Department / Cyber Cell in your Police Station ?	**Yes / No**
2	Is there any sufficient manpower recruited for handling the Cyber Cases in your Police Station ?	**Yes / No**
3	Is there training given to staff by Govt. on cyber crime investigation?	**Yes / No**
3	Is there Trained staff for handling the Cyber Cases?	**Yes / No**
4	Is this staff handles Cyber Cases only? OR they have allotted some other work other than Cyber Cases (please specify)	**Yes / No** **Yes / No**
5	Is the Cyber Cell Well Equipped in all aspects ?	**Yes / No**
6	Is the Cyber Cell using the latest software ?Please specify the name of the software & version	**Yes / No**
7	Is the Cyber Cell using the latest hardware ?	**Yes / No**
8	Do you get CDR [Call Detail Record] immediately from ISPs [Internet Service Providers] in time?[if no please specify the period]	**Yes / No**
9	Problems you have to face while handling following Cyber Crimes? [Please fill up the details]	
	a) Social Networking Crimes [Facebook, Twitter & other sites]	
	b) Credit / Debit / ATM Fraud	
	c) Insurance Fraud	

	d) Job Fraud	
	e) Loan Fraud	
	f) Matrimonial Fraud	
	g) Online Business Fraud	
	h) Hacking (Mail, Website, Data)	
	i) Mobile Offences (Hacking of Mobile Phones , Mobile threatening & extortion)	
10	Do you face any problem in investigation if the person handles the case, get transferred to other location?	**Yes / No**
11	Do you have the authority / powers to resolve the Cyber Crimes ?	**Yes / No**
12	Do you take Support of External Agencies / Experts	**Yes / No**
13	What Legal issues , you have to face at the time of Investigation?	
14	In case of International Cyber Crime , Do you get support from Foreign	

	Countries?	
15	Your expectations from Govt. & Other Authorities? Please specify	
16	Your valuable suggestions for accelerating Cyber Crime Investigation Process	

Name of the Official : ……………………………

Designation : ……………………………………..

Contact No………………………………………..

Seal & Signature …………………………………

* * * * * * * * * * * * * * * * * *

Cyber Safety Awareness program

1. Name of Team Members:
   a) Member 1: ______________________________
   b) Member 2: ______________________________
   c) Member 3: ______________________________

2. Details of School
   a. Name of School: ______________________________
   b. School Address: ______________________________
   c. Phone No.: ______________________________
   d. Email id: ______________________________
   e. Website address: ______________________________
   f. Principal Name: ______________________________
   g. Coordinator Name: ______________________________
   h. Designation: ______________________________
   i. No. of students :

Std.	Total	Attended
V		
VI		
VII		
VIII		
IX		
X		

No of Presentations conducted: Date :

Remark of School principal:

____

____

____

Feedback of School Authority

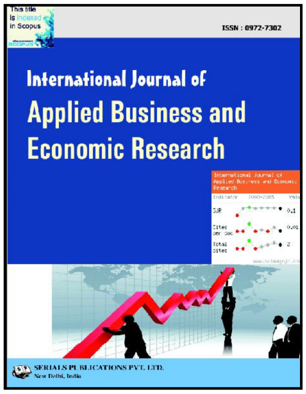
Excellent	Good	Better	Satisfactory

(Note: Tick appropriate)

6. Suggestions

7. No. of CD/DVDs received

Principal's Name & signature: ______________________________



International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournals.com

© Serials Publications Pvt. Ltd.

Volume 15 • Number 16 (Part - II) • 2017

Analysis of Cyber Safety Awareness Amongst Internet Users in Pune

Swati Sayankar[1] and Asha Nagendra[2]

[1] Research Scholar, Tilak Maharashtra Vidyapeeth, Pune (MH), India
[2] Symbiosis Institute of Management Studies, Pune (MH), India

Abstract: Pune city is growing in all aspects may be Educational, Cultural, Industrial etc. due to its conducive environment. Pune being the IT hub of Maharashtra, has been facing a problem of increasing cyber crimes in last 5 years. This fact is supported by NCRB (National Crimes Record Bureau) of India which has highlighted that Cyber crimes in Pune region are increasing at an alarming rate in the last few years. Hence the need of cyber safety awareness while using Internet or advanced technologies becomes sine-qua-non. The purpose of this research paper was to find out the awareness of Internet Users on cyber safety. For this, primary data was collected and analysed from 1122 people who are using Internet and of are of different age groups. It was found that though people are using new technologies such as Internet, Emails, Social networking sites, antivirus, Debit/Credit cards for financial transactions, they are less aware about the do's and don'ts of using these technologies which is a serious threat to the increasing cyber crimes. There is need to inculcate 'Best Practices' amongst this age group so as to reduce quantum of cyber crimes. If this awareness is not created, the rate of cyber crimes will increase which in turn will create burden on 'Cyber Cell' and 'Cyber Forensic labs'.

Keywords: Cyber safety, Cyber crimes, Netiquette, IT Act, IPC

INTRODUCTION

Cyber crime includes all criminal activities done using the medium of communication devices like computers, worldwide web, mobile phones, tablets, internet and cyber space. Any activity that uses computer as an instrument, target or a means for perpetrating crime falls within the ambit of cyber crime.

Understanding cyber safety is more important when one is online. A person may be a working Professional, Teacher, Parent or family member, the knowledge to stay safe online or while using Information Communication Technology (ICT) is a must.

Cyber safety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette). Cybercrime are increasing at an alarming rate. This fact is revealed from the NCRB (National Crimes Records Bureau) of India.

Table 1
Incidence of cases registered under Cyber Crime from 2013-15 under IT ACT (State wise)

SNo	*State*	*2013*	*2014*	*2015*	*Total*
1	Andhra Pradesh	651	282	536	1469
2	Assam	154	379	483	1016
3	Karnataka	533	1020	1447	3000
4	Kerala	383	450	290	1123
5	Maharashtra	907	1879	2195	4981
6	Rajasthan	297	697	949	1943
7	Tamil Nadu	90	172	142	404
8	Telangana	-	703	687	1390
9	Uttar Pradesh	682	1737	2208	4627

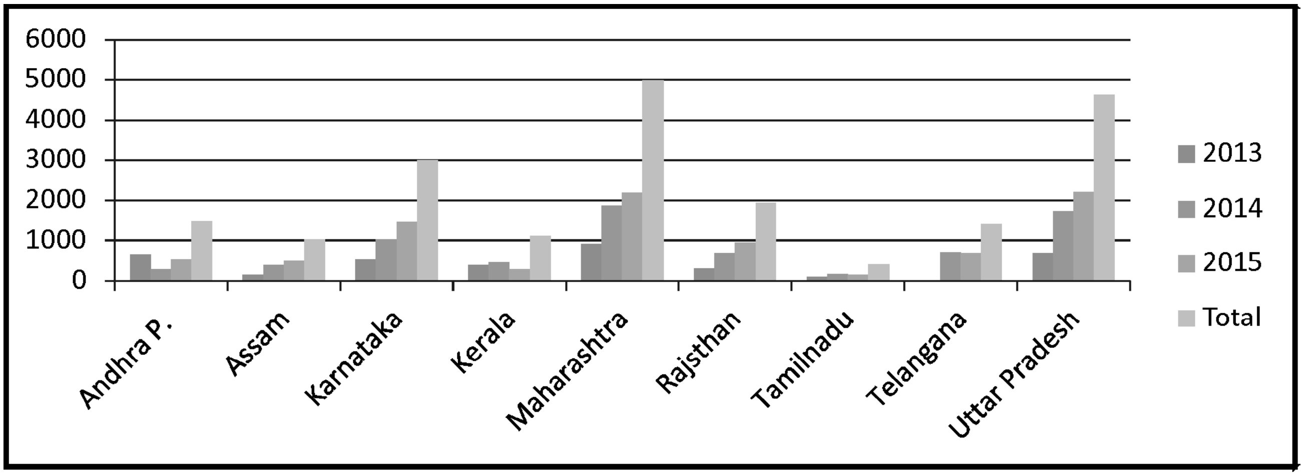


Figure 1: State wise Cyber crimes from 2013-15 in India

The above Table and figure show that in the last 3 years, Maharashtra has the highest no of recorded cyber crimes which is a serious threat to safety and security of Individual, Organisation and state in turn. Pune being the IT and educational hub was therefore considered for the study of cyber safety awareness of people. The observations will help to understand the fact.

REVIEW OF LITERATURE

Report of Cyber Forensic Lab (2009-2011), Santa Cruz (Mumbai)- Maharashtra received from Directorate of Forensic science Laboratories, Home Department, Santa Cruz, Mumbai, Maharashtra under RTI. This report shows trend of rising cyber crimes from 2009 to 2011. The crimes are mostly related to E-mail theft, Data theft, website Hacking, Phishing, Credit card Frauds. There are huge no. of cyber crimes under investigation.

Report of Cyber Cell (2009-2011), Crime Branch, Thane- Maharashtra This report is given by Government Information officer and Asst. Police commissioner, Crime Branch, Thane under RTI. This report highlights cyber crimes related to Data Theft, Phishing, Credit Card Frauds. From 2009-2011, out of 24 cases 16 i.e. approx. 66% cases are under investigation which is a serious threat..

Report of Cyber Crime Cell (2009-2011), Mumbai-Maharashtra received from Cyber Cell, Crime Branch, Mumbai (2012) , given by Government Information Officer and Asst. Police Commissioner, Crime Branch, Mumbai under RTI. This report shows that out of 14 cyber crimes (2009-2011) related to E-mail theft, Data theft, Phishing and Credit Card Frauds, only 4 cases are under investigation which is only 30%.

Report of Cyber Crime Cell (2009-2011), Pune-Maharashtra received from Office of Pune Commissioner and Public Information Officer, Cyber cell, Crime Branch, Pune (2012). This report shows cyber crimes related to Email Threat, Data Theft, Website Hacking, Phishing and Credit card Frauds.

ISO 27001 i.e. ISO27001 is the international Cyber security Standard. It is for managing Information Security System. It provides a prototype for improving, operating establishing, implementing, monitoring, maintaining and reviewing an Information Security System.

Kareem (2015) in his paper on cyber crime investigation, he studies impact of ICT issues on private sectors and e-Governments

Sharma (2012) studied various cyber security emerging trends. These trends he considered as mobile computing, cloud computing, social networking and e-commerce. Dalal (2015) in his research article on Cyber Safety, predicted that state sponsored cyber attacks would increase.

1. OBJECTIVES

1. To identify increasing Cyber crimes in Pune
2. To conduct cyber safety awareness survey of people in Pune
3. To find out probability of risks using Risk assessment Matrix

2. METHODOLOGY

Primary data was collected by the survey method. 2 sets of questionnaires were prepared for collecting data from people.

Questionnaire-1 was filled by personnel from various Cyber cells and Cyber Forensic Lab of Maharashtra for the year 2009-2011.

Questionnaire-2 was filled by the 1122 people of age-group 18-30 on 'Cyber Safety Awareness'.

Questionnaires were designed to study different angles of cyber crime investigation such as frequent cyber crimes, reasons of pending cases, user behaviour while using Internet, Online Banking and other e-transactions, Email, legal aspects etc.

The records of last five years (2011-2016) were collected from various police stations, Cyber Cell in Tabular Format.

Sample size selection was made on the basis of **Morgan table using multistage stratified random sampling.**

Secondary data was collected from the website of National Crime Record Bureau of India.

Data analysis has been performed using **SPSS-21 and Microsoft excel.**

3. AWARENESS OF PEOPLE IN PUNE ON CYBER SAFETY

To identify internet users, the following questions were asked to 1122 respondents.

Q.1) Do you have an email account?

Table 2
Table showing % of Internet users who have email account

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	1065	94.9	94.9	94.9
	No	57	5.1	5.1	100.0
	Total	1122	100.0	100.0	

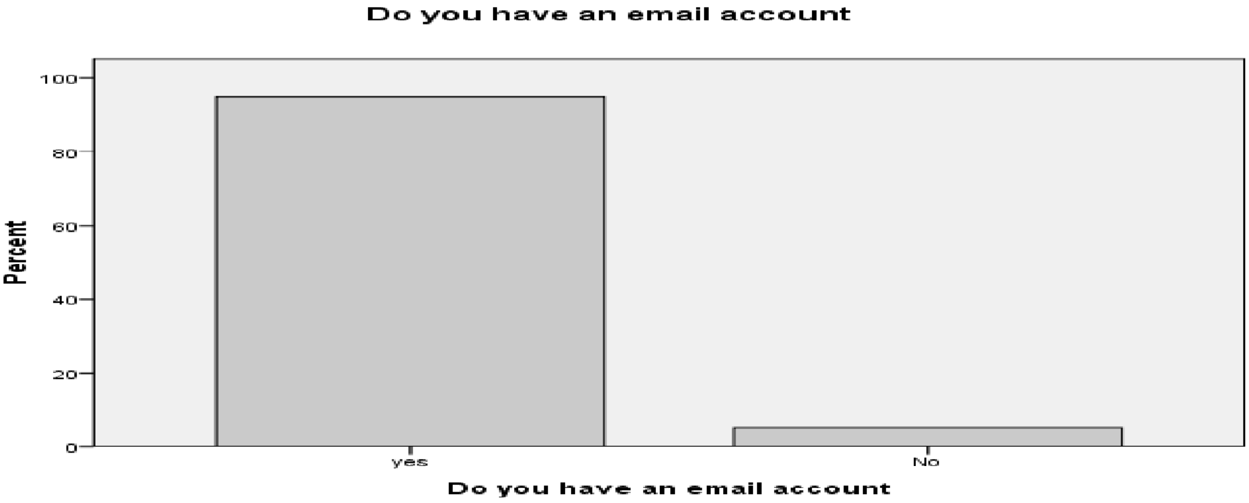


Figure 2: Internet users having an email account

The above frequency distribution table shows that from selected Sample, there are 94.9 % people who are using an email account. Only 5.9% people do not have an email account.

This was the reason why the survey of internet users on "cyber safety awareness" was carried out. Considering various most frequent cyber crimes as reported by NCRB (National Crime Records Bureau of India) related questions were asked to internet users. This will give an idea to researcher about level of awareness amongst internet users.

Q.2) Is your password strong?

Table 3
Strong password

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	Alphabet	267	23.8	23.8	23.8
	Number	176	15.7	15.7	39.5
	Special characters	27	2.4	2.4	41.9
	Alpha numeric	261	23.3	23.3	65.2
	Combination of all	391	34.8	34.8	100.0
	Total	1122	100.0	100.0	

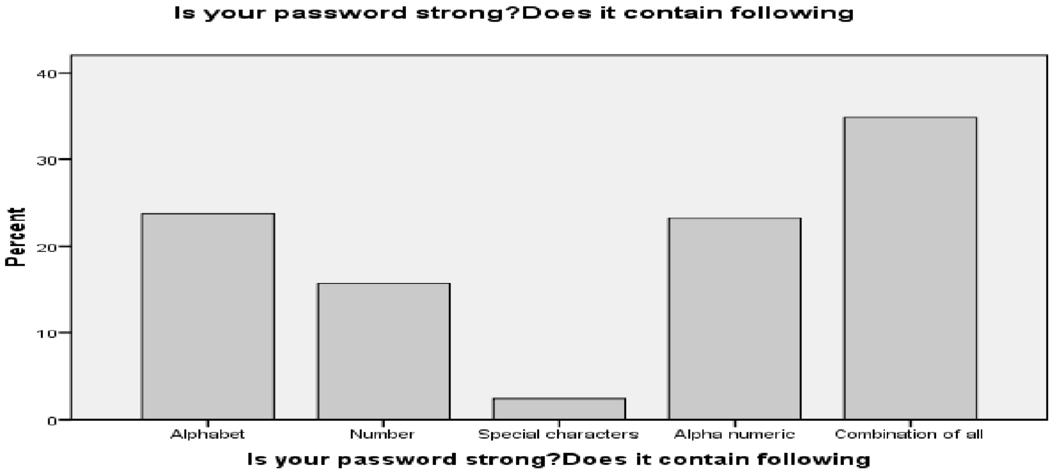


Figure 3: Is your password strong?

From the above figure and table, it can be seen that out of 1065 respondents only 391 users i.e.34.8% people have strong password that contains alphabets, numbers, special characters etc. The strong password is required to protect the system from unauthorised access to data or information. Therefore risk level observed falling to cyber crime is high.

Q.3) Which social networking sites do you use?

Table 4
Use of Social networking sites

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	facebook	529	47.1	47.1	47.1
	twitter	40	3.6	3.6	50.7
	whatsApp	436	38.9	38.9	89.6
	any other	60	5.3	5.3	94.9
	nothing	57	5.1	5.1	100.0
	Total	1122	100.0	100.0	

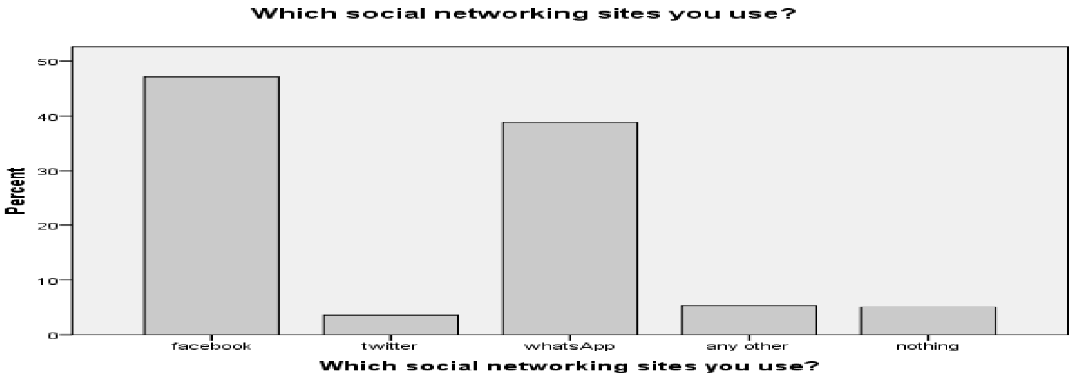


Figure 4 : Use of Social networking sites

From the above frequency distribution table it can be observed that out of 1065 internet users 529 (47.9%) people use Facebook, 436(38.9%) people use WhatsApp and 40 (3.6%) people use Twitter.

It shows that mainly 94.96% people use Facebook, WhatsApp, Twitter and other social networking sites. Hence it becomes necessary to know the Do's and Don'ts while using above media.

Q.4) Do you have different password for email and social media accounts?

Table 5
Different password for email and social media accounts

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	819	73.0	73.0	73.0
	no	303	27.0	27.0	100.0
	Total	1122	100.0	100.0	

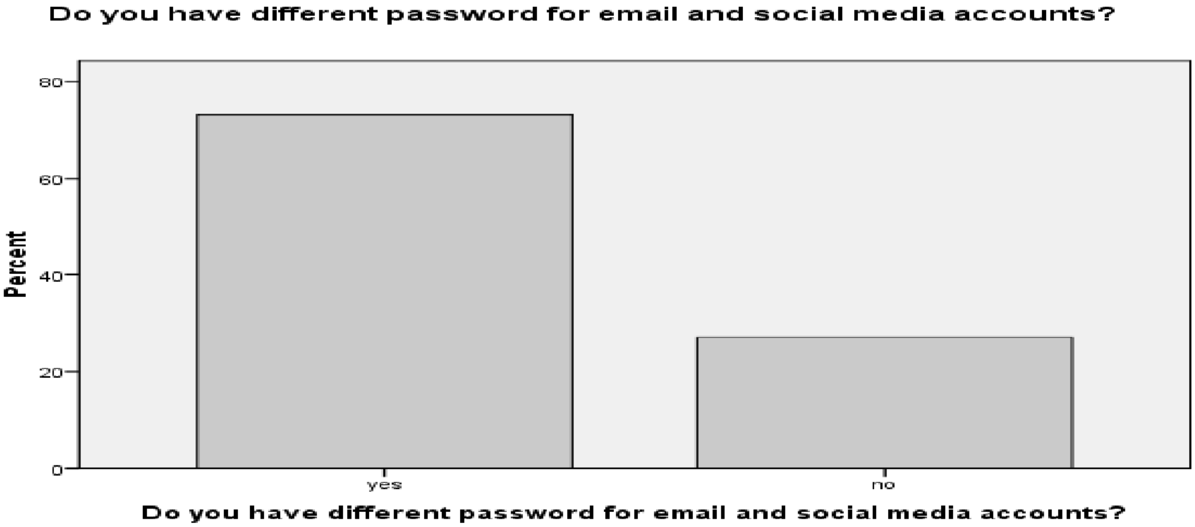


Figure 5: Different password for email and social media Accounts

From the above Frequency table it can be seen that 73% users have different passwords and 27 % users have same password for email and social media accounts which is a threat to cyber safety of these users.

This helps the Hacker to use same password for different accounts and obtain the sensitive information such as Banking details, credit/debit card details, personal information. This may lead to money loss, loss of confidential information of individual or organisation, defamation etc.

Q.5) Have you uploaded following personal details on social networking sites?

Table 6
Personal Details on Social Networking Sites

	Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Your photo	326	29.1	29.1	29.1
contact no.	35	3.1	3.1	32.2
Email	163	14.5	14.5	46.7
Address	12	1.1	1.1	47.8
All	432	38.5	38.5	86.3
Nothing	154	13.7	13.7	100.0
Total	1122	100.0	100.0	

		Frequency	*Per cent*	*Valid Per cent*
Valid	Yes	53	4.7	4.7
	No	815	72.6	72.6
	sometimes	254	22.6	22.6
	Total	1122	100.0	100.0

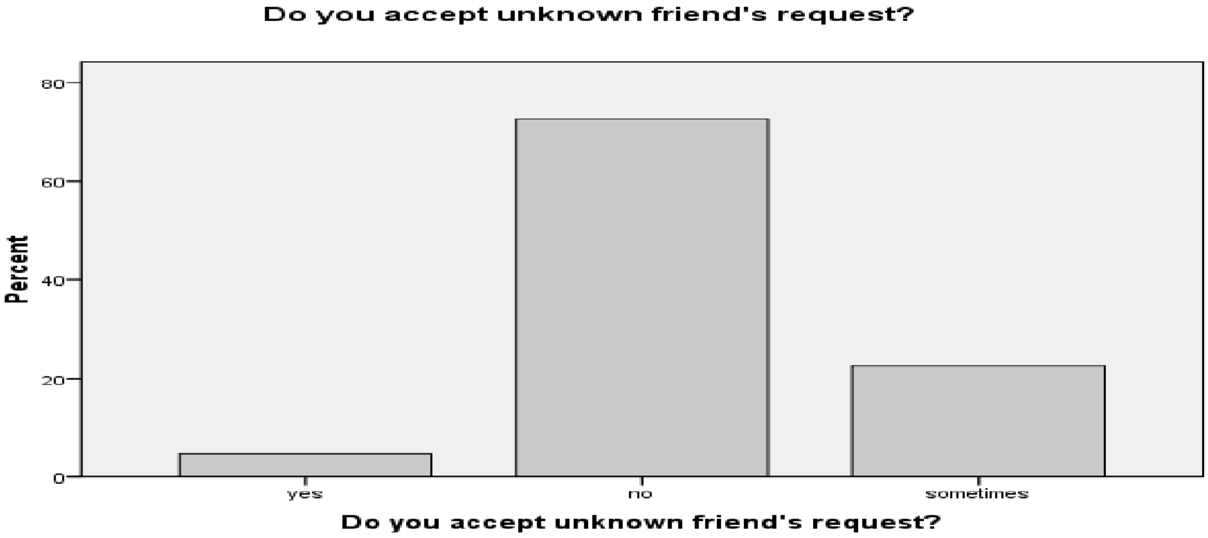


Figure 6: Accepting unknown Friend's Request

From the above Frequency table it can be seen that out of 1122 users, 4.7 % people accept request. 72.6% users not accepting request. But sometimes 22.6% users accept request is a big risk and may fall victim to cyber crimes.

Q.7) Have you installed Antivirus and Firewall on Your PC?

Table 8
Installing Antivirus and Firewall on Your PC

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	installed antivirus only	509	45.4	45.4	45.4
	installed firewall only	35	3.1	3.1	48.5
	installed both-antivirus and firewall	344	30.7	30.7	79.1
	installed none	234	20.9	20.9	100.0
	Total	1122	100.0	100.0	

From above Frequency Distribution Table it can be seen that out of 1122 users 509 users have installed Antivirus, 35 have installed only Firewall and 344 people have installed both. But There are 234 people who have not installed antivirus or Firewall. Therefore it may create big risk as system may fall to data loss, data modification due to virus attack.

Q.8) Do you know IMEI of your mobile Phone?

Table 9
Knowing IMEI of your mobile phone

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	479	42.7	42.7	42.7
	no	643	57.3	57.3	100.0
	Total	1122	100.0	100.0	

Above Frequency Distribution table shows that out of 1122 mobile users, only 42.7 % people know IMEI of their Mobile phone. This is a serious threat as your mobile has important personal and official contact numbers and other files, photos and SMSs.

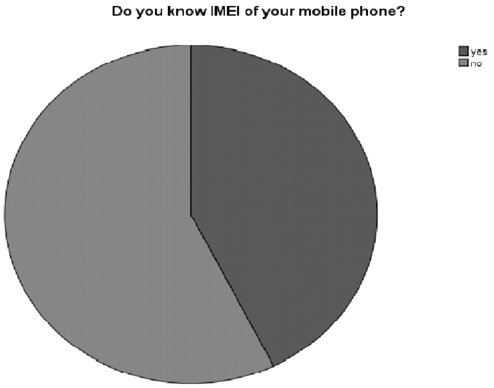


Figure 7: Knowing IMEI of your mobile phone

It can be seen from above graph 57.3 % people do not know IMEI no. of their Mobile. In case of mobile theft or loss of mobile, IMEI no helps Police, Investigation office to track mobile, block the details so that no one can use the data / information from stolen mobile. Hence there is need to create awareness amongst users to know IMEI to save important information stored on Mobile device.

Q.9) Do you note down ATM card and customer service no on your mobile?

Table 10
Noting down of ATM card and customer service number on respondent's mobile?

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	Yes	759	67.6	67.6	67.6
	No	363	32.4	32.4	100.0
	Total	1122	100.0	100.0	

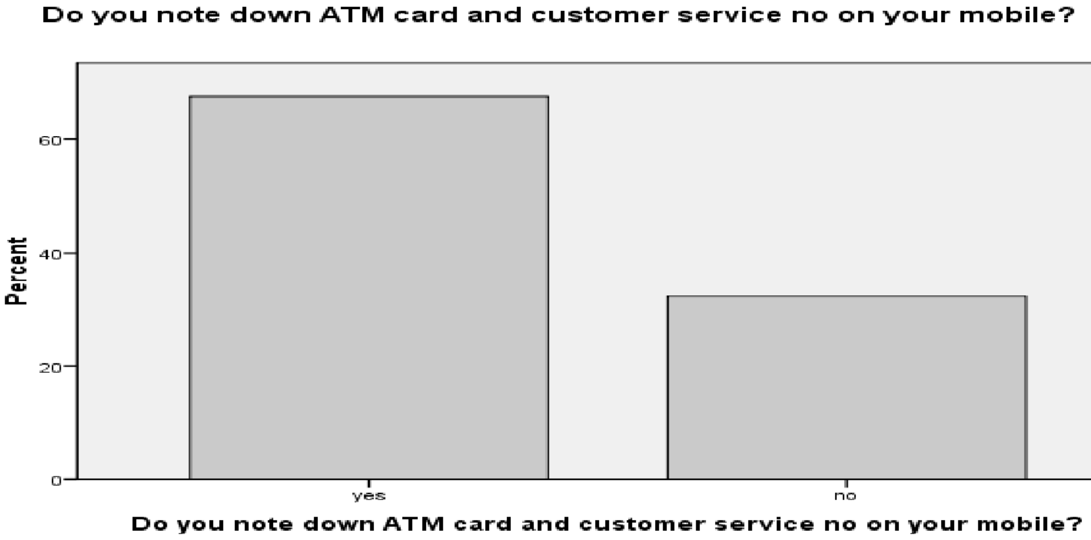


Figure 8: Noting down of ATM card and customer service number on respondent's mobile

Noting down ATM card and customer service number on their mobile may lead to data loss, loss of money through banking transactions.

Q.10) Do you store your password, pin in your mobile as contact number?

Table 11
Storing password, pin in respondent's mobile phone as contact number

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	258	23.0	23.0	23.0
	no	864	77.0	77.0	100.0
	Total	1122	100.0	100.0	

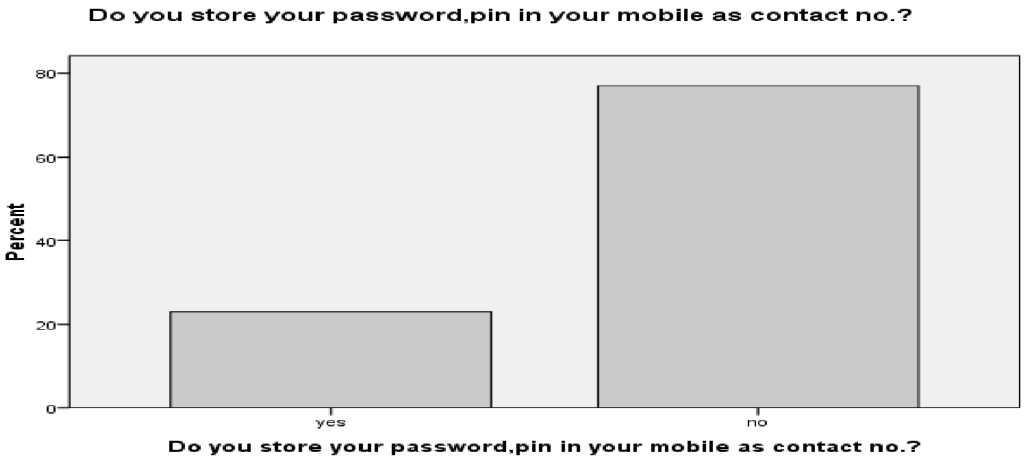


Figure 9: Storing password, pin in the mobile phone as contact number

From the above data, it is seen that 258 people are storing password, PIN on their mobile. This may lead to data loss, loss of money through banking transactions. From Q.9 and Q. 10 it can be observed that storing such sensitive information such as ATM no, Customer service no., password, PIN no is big threat and may lead to cyber crimes.

Q.11) Do you receive email/SMSs / phone calls that promise large sum of money/discounts?

Table 12
Respondents receiving email /SMSs/ phone calls

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	596	53.1	53.1	53.1
	no	526	46.9	46.9	100.0
	Total	1122	100.0	100.0	

Out of 1122 people, 53.1% people are getting such emails /SMSs/ phone calls. This is a significant percentage (being above 50%) and needs special attention and awareness of Individual and Government. The respondents were further asked whether they respond to such mails or SMSs/ phone calls.

Q.11 .1) If Yes, do you respond ?

Table 13
Responding to such calls

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	149	13.3	13.3	13.3
	no	973	86.7	86.7	100.0
	Total	1122	100.0	100.0	

Out of 53.1% people, 13.3 people respond to such emails or SMSs or phone calls. Their method of responding also surveyed further by asking following question.

Q.11.2) If yes, how do you respond?

Out of 266 people, 130 (11.6%) people reply to SMS/email, 60 (5.3 %) people call back to emails or phone numbers or SMSs and 76 (6.8 %) people entertain unknown calls which are a serious threat. They may fall victim to Cyber crimes such as Nigerian Fraud, Phishing scams, Identity Theft etc.

Table 14
Ways of responding to unknown calls

If yes, then how you respond?

	Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
By replying to SMS/email	130	11.6	11.6	11.6
By calling contact no.given in email/sms	60	5.3	5.3	16.9
By entertaining their call	76	6.8	6.8	23.7
not applicable	856	76.3	76.3	100.0
Total	1122	100.0	100.0	

4. RISK ASSESSMENT TABLE

It is a step in a procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard).

We are specially studying Risk assessment with reference to cyber security. This will help in analyzing factors affecting effective investigation of cyber crimes. There are two types of Risk Assessments·

1) Quantitative Risk Assessment

2) Qualitative Risk assessment

Qualitative risk assessment comes into play when we have the ability to map an amount to a specific risk. Qualitative Risk assessment typically give risk results of 'High', 'Moderate' and 'Low'. By providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization.

Table 15
Risk Assessment Matrix

RISK ASSESSMENT MATRIX			
	H/M/L	H/M/L	H/M/L
MOTIVATION	HIGH	HIGH	LOW
CAPABILITY	HIGH	HIGH	MODERATE
CONTROLS	LOW	MODERATE	HIGH
RISK LEVEL	HIGH	MODERATE	LOW

(P.N. above Risk Assessment Matrix is as per Microsoft's Information Security Standards)

After studying cyber safety awareness various other factors through different questionnaires, following **Risk Matrix** is prepared. This Risk matrix shows Risk levels before and after implementing security measures or Controls.

Risk Assessment Table is based on Microsoft's Risk assessment matrix. This Qualitative Risk assessment typically gives risk results of 'High', 'Moderate' and 'Low'.

By providing the impact, it is possible to adequately communicate the assessment of risk to individual or the organization. This Risk Assessment Table highlights the possibility of cyber crimes based on risk level. This table highlights the fact that there is need to inculcate cyber safety rules awareness amongst users who are using new technologies and internet.

Firstly, the Vulnerabilities are identified. Vulnerability is nothing but a weakness in the system which gives an attacker a chance to attack or hack a system. Based on the responses received from the questionnaire, Risk Assessment Table is prepared.

Table 16
Risk Assessment Table

S.No.	*Vulnerability Gateways for cyber crimes (How it may happen)*	*Yes (%)*	*No(%)*	*Risk level H/L/M*
1.	Strong password (Threat: Majority of the users (65%) do not have strong password.)	34.8	65.2	**H**
2.	Different passwords for email and social networking accounts (Threat: Good to have different passwords. But People may forget passwords. If stored on mobile or database it may be hacked. 27% people are using same passwords which is risk to their social networking accounts)	73%	27	**H**
3.	Accepting Unknown Friends Requests (Threat: Carry risk of personal and social life.)	27.3	72.6	**H**
4.	Installing Antivirus and Firewall both (Need to create awareness amongst 70% people about use of Firewall.)	30.7%	69.3	**H**
5.	Knowing IMEI of your mobile (Helps in Mobile theft. Not knowing IMEI may lead to hack personal information/ Financial loss)	42.7	57.3	**H**
6.	Storing Password / PIN on mobile phone as contact number (In case of mobile theft, details are used by cyber criminals)	23.0	77.0	**M**
7.	Receiving Emails/SMSs/ Phone calls that promise large sums of money /discounts (Gateways for cyber crimes of those who respond)	53.1	46.9	**H**
8.	Responding to such calls	13.3	86.7	**M**
9.	Uploading personal details on Social websites(May lead to personal/ Financial/Social loss)	47.8	52.2	**H**
10.	Way of responding to calls (by SMS/Email/Call/entertain suchcalls)	23.7	76.3	**M**
11.	Accepting unknown friend's request (Risk of cybercrimesincreases)	27.3	72.7	**H**
12.	Noting ATM card and Customer service number on their Mobile phones	67.6	32.4	**H**
13.	**Awareness about terms**			
	Nigerian Frauds	0.6	99.4	**H**
	Credit card frauds	11.1	88.9	**H**
	Phishing	2.7	98.3	**H**
	Identity Theft	5.7	94.3	**H**
	Hacking	38.8	61.2	**H**
	All above	32.8	67.2	**H**
	(Threat:Very less awareness may give birth to Cyber crimes)			

(P.N. Yellow mark highlights risk level High)

Above Risk Assessment Table shows level of Cyber Safety awareness amongst Internet users in terms of Percentage. It is further marked in terms of Risk level which is High or Medium. The percentage highlighted in yellow indicates that there is less awareness related to general awareness while using internet, computers, mobiles, ATM etc. The above table shows that awareness of cyber safety amongst Internet users is less and may give rise to cyber crimes in future.

5. FINDINGS

From above research, following findings have been derived.

1) Majority of respondents (94.5%) now a days are using Internet and email accounts.
2) Password of accounts is not strong amongst 65.2% people.
3) 95% from that use social networking sites
4) 73% respondents use same password for different accounts which is arisk,
5) Almost 48% respondents upload personal details (Photo, Contact number, email, address) on social networking sites which is a risk.
6) Only 45% respondents installed Antivirus on their Computers.
7) 57.13% respondents don't know IMEI of their mobile.
8) 67.6% repondents take a risk to note down ATM and customer service number on mobile.
9) 23% respondents store password, PIN in mobile.
10) 53% respondents receive unknown calls (emails, SMSs, phone calls that promise large sums of money.
11) 23% respondents reply to unknown calls.

6. CONCLUSION

1) Observations on 'Technology awareness' and 'Cyber Security Risk Analysis Report' between the age group of 18-30 based on survey in Pune region reveals that there is a great need to conduct 'Proactive Awareness Campaign' on 'Cyber Safety'.
2) Though people are using new technologies such as Internet, Emails, Social networking sites, antivirus, Debit/Credit cards for financial transactions, they are less aware about do's and don'ts of using these technologies which is a serious threat to increase cyber crimes.
3) There is need to inculcate 'Best Practices' amongst this age group so as to reduce quantum of cyber crimes.
4) If this awareness is not created, the rate of cyber crimes will increase which in turn will create burden on 'Cyber Cell' and 'Cyber Forensic labs'.

This will affect the effective investigation of cyber crimes in Pune region. The period to resolve registered cyber crimes will increase which is a boon for Cyber criminals.

7. MANAGERIAL APPLICATIONS

1) College students can be trained by experts on 'cyber Safety Awareness'. Theses students can conduct presentations in schools and colleges to spread cyber literacy.

2) ERP Software for effective cyber crime investigation process can be developed that will save time for manual work related to cyber crimes investigation and will link all Cyber Cells in the Country.

8. SCOPE OF FUTURE WORK

1. The present research is carried out in Pune region but is must for every city in Maharashtra and also other states of India.

2. Yearly Cyber safety Literacy survey of every city can be done in India.

3. Research on 'Cyber Safety and Security Policies' of different organizations can be done.

REFERENCES

Crime Statistics 2011-2016. (n.d.). Retrieved April 25, 2017, accessed from http://www.ncrb.org

Growing Cyber Security-Industry-Roadmap for India. (n.d.). Retrieved July 20, 2016, from https://www.dsci.in/content/studies-reports

Kadam, A. (2012). Network Security-Defense in Depth. Geographic India System, 35(10), ISSN 0970-647x, 30-31.

Kadam, A. (2012). Physical Security -Defense in Depth. Geographic Information System (GIS),35(11), ISSN 0970-647x, 36.

Kadam, A. (2012). Information Security- Personnel Security-|Defense in Depth. Data Compression,35(12), ISSN 0970-647x, 30-31.

Kothari, C. R., &Garg, G. (2014). Research Methodology-Methods & Techniques(3rd ed., Vol. 3, ISBN:978-81-224-3623-5). New Delhi, Maharashtra: New Age International (P) Ltd.

Mali, P. (2012). Data Loss Prevention (DLP). Geographic Information System (GIS),35(11), ISSN 0970-647x, 35.

Mali, P. (2013). Cyber Law and cyber crimes(1st ed., Vol. 1, ISBN:978-81-8159-574-4). Mumbai, Maharashtra: Snow White.

Mali, P. (2013). Cyber law and cyber crimes(1st ed., Vol. 1, ISBN:978-81-8159-574-4). Mumbai, Maharashtra: Snow white.

Nagpal, R. (n.d.). Evolution of Cybercrimes. Retrieved May 25, 2015, from http://www.cyberlawdb.com/docs/ebooks/cc.pdf

Online Safety Tips. (n.d.). Retrieved June 10, 2016, from http://www.punepolice.gov.in/content/cyber-crime-cell-awareness-notes

Paranjape, V. (2010). Legal Dimensions of Cyber crime and Preventive Laws-with special reference to India(1st ed., Vol. 1). Allahabad, Uttar Pradesh: Central.

Parthsarthi, P. (2012). Cyber crimes. Retrieved January 15, 2016, from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

Sood, V. (2010). Cyber Crime, Electronic Evidence & Investigation Legal Issues(1st ed., Vol. 1, ISBN-978-81-7274-707-7). New Delhi, Uttar Pradesh: Nabhi Publication.

W. (n.d.). Understanding Cyber crimes, Computer Forensics and Legal Perspectives (1st ed., ISBN: 978-81-265-2179). Wiley India Pvt. Ltd.

Proactive Implementation of “Information Security Awareness Program” for Netizens of Maharashtra – a need of Government initiative to combat rising cyber crimes in Maharashtra.

Swati Sayankar

Research Scholar - Tilak Maharashtra Vidyapeeth,Pune

E-mail : swatisayankar@rediffmail.com

Abstract: **This research paper aims at implementation of ‘Information Security Awareness program’ for preventing Cyber crimes for Netizens of Maharashtra who are constantly communicating through cyberspace. Findings on “Cyber Crimes Statistics’ obtained from National Crime Records Bureau (NCRB) of India and various reports obtained from many cyber cells and cyber forensic Laboratories of Maharashtra on cyber crimes (2009-11) suggests to implement Security Awareness Program for stakeholders of Internet in various sectors of Maharashtra. This paper recommends Government’s attention to implement ‘Security Awareness’ program on priority basis to minimize cyber crimes in Maharashtra.**

Keywords: Netizens, Stakeholders, Cyber space, White Collar criminals

1 Introduction

With emergence of new communication Technologies called ‘Information Communication Technologies’ and their adaption in day today life by people in various sectors gave rise to new types of crimes called ‘Cyber crimes’ done through Cyber space by white collar criminals. The adaption of these technologies without implementing ethics called cyber ethics gave birth to Cyber crimes.

Symantec India [1] and National Crime Records Bureau of India publishes annual reports on cyber crimes which shows there is significant rise in cyber crimes during 2009-11 which have been committed with different motives from different types of suspects by various age groups from various sectors of society.

In support of these findings, specific reports are obtained from Cyber forensic Lab and Cyber Crime Investigation Cells of Maharashtra (Santacruz ,Prune, Mumbai, Thane) which highlights most frequent cyber crimes. Most of these crimes are committed due to the problem of lack of Information Security Awareness amongst people because of which they are falling victims to cyber crimes.

2 Identification of Problem

After studying the reports of NCRB from the year 2009-11, we come to know that cyber crimes in Maharashtra in cities like Pune, Mumbai, Nagpur, Nasik and Aurangabad are highest compared to other states.

Further statistics of NCRB [2] on cyber crimes highlights following facts with reference to Maharashtra as follows.

1) Incidence of cases registered on cyber crimes during 2009-11 in Maharashtra are highest compared to other states.

Table 1. Cyber crimes in Maharashtra

State	Cyber crimes
Maharashtra	501
Andhra Pradesh	484
Kerala	439
Karnataka	401
Rajsthan	201

2) Pune, Delhi, Bengaluru, Vishakhapattanam have highest record of cyber crimes in 2011. Cyber crimes are notable in these cities.

Table 2. Cyber crimes in cities of India in 2011

State	Cyber crimes
Pune	83
Delhi	50
Bengaluru	117
Vishakhapattanam	107

3) State wise person arrested during 2009-11under IT Act by age group of 18-30 is highest compared to age group 30-45.

Table 3. Person arrested under cyber crimes(2009-11)

State	Person arrested (18-30 age group)	Person arrested (30-45 age group)
Andhra P.	173	135
Maharashtra	278	155
Kerala	172	68
Madhya P.	10	62

This is serious problem as Youth of this country is mainly involved in this.

4) City wise persons arrested under IT Act by age group 18-30 and 30-45 during 2009-11 is as follows.

Table 4. City wise persons arrested (2009-11)

City	Age group (18-30)	Age group (30-45)
Pune	34	22
Bengaluru	26	21
Hyderabad	30	20
Bhopal	23	7
Delhi	26	11

5) Incidences of cases registered in 2009 under IT ACT under different crimes heads (all-India)

Table 5. cases registered under diff. crime heads

Crime Head	Cases Registered	Persons Arrested
Loss/Damage to Comp Resource	115	63
Hacking	118	44
Obscence Publication in electronic form	139	14
Total	414	154

6) In 2009, In Andhra Pradesh, Kerala, Maharashtra, Rajsthan cyber crimes due to Loss or damage are notable. **Table 6.** Statewise loss or damage

State	Tempering source code	Loss/ Damage	Hacking	Obscene Publication
Andhra P.	7	267	20	52
Karnataka-ka	0	81	23	37
Kerala	6	55	22	136
Maharashtra	7	68	11	62
Rajsthan	12	69	0	40

7) Maharashtra is highest in committing cyber crimes by all motives (Revenge, Fraud,extortion, fraud, greed etc.).

Table 7. Cases registered under cyber crimes by all motives (state wise) during 2009-11

City	2009	2010	2011	Total
Maharashtra	161	246	393	800
Andhra Pradesh	38	171	372	581
Kerala	71	156	245	472
Karnataka	97	176	160	433
Chattisgadh	50	50	78	178
Madhya Pradesh	17	35	103	155
Total	434	2844	1351	2619

8) Maharashtra has highest no. of suspects during 2009-11. These suspects include Foreign/National, disgruntled employees, students, professionals, business competitor, neighbors, relatives etc.

Table 8. State wise suspects (2009-11)

City	2009	2010	2011	Total
Maharashtra	161	246	393	800
Andhra Pradesh	38	171	372	581
Kerala	71	156	245	472
Karnataka	97	176	160	433
Chattisgadh	50	50	78	178
Madhya Pradesh	17	35	103	155
Total	434	2844	1351	2619

3 Findings

From above reports it is clear that Cyber crimes in Maharashtra are notable. Therefore reports from Cyber forensic lab and cyber cells of Maharashtra are collected which provides following facts to strengthen research statement.

Report 1) Forensic Science Laboratories, Santacruz: [3]

This Report states that e-mail thefts, Data theft, Website hacking, Phishing, Credit card frauds in the year 2009, 2010, 2011 are 171, 270, 345 respectively. This shows that there is rise in above mentioned crimes.

Report 2) Cyber crime Investigation Cell, Thane, Mumbai: [4]

This Report states Total cyber crimes related to Data Theft, Phishing, Credit Card frauds, email threats and Website hacking are 66, 4, 35, 27, 0 respectively during 2009-11

This report also shows that crimes reported under section 66 A,B,C,D are more compared Section 65 and 67as mentioned in IT (Amendment) Act 2008.

Report 3) Cyber crime Investigation Cell, Mumbai: [5]

Email threats reported by this Crime Investigation cell are 4,1,2 in the year 2009, 2010,. 2011 respectively. Similarly data thefts registered are 2, 0, 1 in the year 2009, 2010,. 2011 respectively.

Report 4) Cyber crime Investigation Cell, Pune :[6]

Phishing and Credit card thefts are more in Pune in 2009-11. Along with this email thefts, website hacking, Data thefts are rising in last 3 years.

4 Problem analysis

The frequency of cyber crimes related to Phishing, Credit card Thefts , Data Theft, email threats , Website hacking highlights following facts :

1) Personal information is not cared by netizens. It is produced as response to unknown emails.
2) Unknown attachments are not scanned which allows virus to enter into system via email. Such emails are responded as they pretend to be send from authentic websites or emails.
3) Password is simple not strong which is easy to guess. Also it is not changed periodically.
4) Credit card details are produced to online shoppers. Fake bank- emails.

5) No antivirus software installed on Personal or Network PCs which allows virus intrusion in computers/Network system.
6) Softwares are not licensed.
7) Organizations are not protecting websites, which allows defamation or financial loss to organizations.

Above mentioned negligence is responsible for falling victim to cyber crimes and cyber terrorism in state.

5 Solution

As cyber criminals generally find out the computers / Networks which are weak in security or with security flaws , they send virus programs through emails which traps people who are not aware about Information Security aspects. Unfortunately the number of people who use ICT devices are less aware about their security aspects.

Following are the solutions which when implemented will avoid falling victims to Cyber crimes.

1) Personal information should be protected such as user ids and passwords, credit card numbers, ATM card's PIN and password should not be stored on mobiles or computers or should not be shared.
2) Organizations should secure their websites.
3) License copies of Softwares should be purchased from standard Companies.
4) Do not use pirated softwares,
5) Do not expose your personal details to unknown through social networking sites such as facebook, orkut, twitter etc. Do not send your photographs. Also do not share your personal mobile no. to any one.
6) Do not pass any controversial statement /comment through social networking sites which will harm others.

6 Conclusion

Cyber Terrorism or Terrorists attacks on states through cyber space are cause of worry for every citizen.

Government should take active initiative to implement 'Information Security Awareness program' for netizen of Maharashtra. Data Security council of India (DSCI)and NASSCOM are taking initiative on this. Still effective implementation through compulsory programs on security for all sectors in Maharashtra by all Cyber crime Investigation Cells of Maharashtra, Government authorities of Crime branch is needed which will keep Maharashtra's cyber crime to minimum.

This research paper suggests Cyber crime prevention through 'Information Security Awareness Program' on top agenda of Government for safety and security of Maharashtra state.

7 References

[1] Symantec Internet Security Threat Reports
From 2009-2011

[2] Cyber crime Reports of 'National Crime Records
Bureau of India' from 2009-2011

Cyber Crime reports (2009-11) from

[3] Directorate of Forensic Laboratories,
Santacruz, Mumbai

[4] Cyber crime Investigation Cell,
Thane, Mumbai (India)

[5] Cyber crime Investigation Cell, Mumbai

[6] Cyber crime Investigation Cell, Pune

Adaption of Cyber Ethics – an Effective way to prevent Cyber Crimes [Study with reference to Maharashtra]

Swati Sayankar

MKSSS's K.B.Joshi Institute of IT, Pune (Affiliated to S.N.D.T. Women's University, Mumbai),

Maharashtra (India)

swatisayankar@rediffmail.com

Abstract : **Cyber crimes have increased tremendously in last ten years all over the world. In Maharashtra, the cyber crimes are on rise in last 3 years (2009-11). There is delay in cyber crime investigation process as there are huge receipts of cases all over Maharashtra in cyber Forensic lab and Cyber crime Investigation cells. Delay in cyber crime investigation process is strengthening cyber criminals. Knowing the Cyber Ethics and following Netiquettes , there are less chances of falling victim to cyber crimes which indirectly leads to safe dealing in cyber space. This research paper suggests to adapt Cyber ethics, an effective way to minimize and prevent cyber crimes in Maharashtra.**

Keywords: Ethic, Computer Ethics, Cyber Crimes

1 INTRODUCTION

1.1 ETHICS

Ethics is derived from the Greek word "Ethos", which means "The discipline and practice of applying value to human behavior, resulting in meaningful conduct. "

Ethical behavior results in progress, prosperity and peace in society. Disobeying the code of conduct or unethical behavior results in crimes in society.

1.2 CYBER ETHICS

Applying the same principal of general ethics , Cyber ethics can be defined as " Social code of conduct while surfing on the Internet in cyberspace so as to prevent yourself and your family from becoming victims of cyber crimes ". This code of conduct is also called as 'Netiquettes'- (derived from Internet + etiquettes) .

Computer ethics defined as the application of classical ethical principles to the use of computer technology.

The Ten Commandments of computer ethics have been defined by the Computer Ethics Institute as follows. [1]

Thou Shalt

1) Not use a computer to harm other people.
2) Not interfere with other's computer work.
3) Not snoop around in other people's files.
4) Not use a computer to steal.
5) Not use a computer to bear false witness.
6) Not use/copy s/w for which you haven't paid.
7) Not use other people's computer resources without authorization.
8) Not appropriate other people's

Intellectual output.

9) Think about the social consequences of the Program you write.

10) Use a computer in ways that show Consideration and respect.

2 PROBLEM IDENTIFICATION

Cyber crimes are increasing at an alarming rate with the use of Information Communication Technology (ICT) all over the world. This is not restricted to person or Individual but has covered group, society and country. Cyber Terrorism is largest outcome of cyber crimes committed through cyberspace. Its effects are harmful to developed and developing countries.

3 CYBER CRIMES IN INDIA AND MAHARASHTRA

Cyber Crimes statistics from 2009-11 in India as follows:[2]

1. Cyber crimes in India during 2009-11 are 3058 in all states
2. Cyber crimes in Maharashtra are 501 during 2009-11
3. Person arrested under IT Act during 2009-11 in all states of India are 2217 while in Maharashtra are 247 which is highest compared to other states.
4. Incidences of cases registered of cyber crimes in India in all states during 2009-11 are 4231 while persons arrested are 3374.
5. Incidences of cyber crime cases registered during 2009-11 in India as follows

Table 1. Cases registered under different crimes Heads (India)

Crime Head	India		
	2009	2010	2011
Tampering of Source code documents (Section 65)	21	64	94
Loss/damage (Section 66-1)	115	346	826
Hacking (Section 66-2)	118	164	157
Obscene Publication in electronic form.(67)	139	328	496

Table 2. Cases registered under different crimes Heads (Maharashtra)

Crime Head	Maharashtra		
	2009	2010	2011
Tampering of Source code documents (Section 65)	1	6	7
Loss/damage (Section 66-1)	25	31	68
Hacking (Section 66-2)	0	13	11
Obscene Publication in electronic form.(67)	25	61	62

6. **Report from Forensic Science Laboratories, Santacruz:** [3]

This Report states that E-mail thefts, Data theft, Website hacking, Phishing, Credit card frauds in the year 2009, 2010, 2011 are 171, 270, 345 respectively. This shows that there is rise in above mentioned crimes.

7. **Report from Cyber crime Investigation Cell, Thane, Mumbai:** [4]

This Report states Total cyber crimes related to Data Theft, Phishing, Credit Card frauds, email threats and Website hacking are 66, 4, 35, 27, 0 respectively during 2009-11.

This report also shows that crimes reported under section 66 A,B,C,D are more compared Section 65 and 67as mentioned in IT (Amendment) Act 2008.

8. **Report from Cyber crime Investigation Cell, Mumbai:** [5]

Email threats reported by this Crime Investigation cell are 4,1,2 in the year 2009, 2010,. 2011 respectively. Similarly data thefts registered are 2, 0, 1 in the year 2009, 2010,. 2011 respectively.

9. **Report from Cyber Crime Investigation Cell, Pune :** [6]

Phishing and Credit card thefts are more in Pune in 2009-11. Along with this email thefts, website hacking, Data thefts are rising in last 3 years.

4 PROBLEM ANALYSIS

By analyzing above cyber crimes statistics during 2009-11 in Maharashtra with reference to phishing, credit card frauds, email, thefts, data theft, website hacking etc. this research paper highlights the need to adapt Cyber ethics by Netizen.

5 UNETHICAL ISSUES IN CYBER CRIMES

Unethical issues related to above mentioned most frequent cyber crimes are as follows.

A) Hacking

i) Hacking is an unauthorized attempt to bypass the security mechanism of an information system or network.

ii) Stealing Usernames, Passwords, Credit card information for obtaining personal or financial data

iii) Hackers use faulty Hardware or Software to enter a computer system/network.

B) Data Theft

i) It is stealing information in the form of downloads, copies of extracts of any data without permission of owner

ii) It is Id related theft (Customer records) or company’s intellectual property or proprietary information.

iii) Copying files without permission in pen drive is also data theft.

C) Phishing

i) It is criminally fraudulent process of attempting to acquire sensitive information in the form of username, password, credit card information.

ii) Email are send by phishers that appear to come from legitimate websites.

iii) In this someone pretends to be someone else.

iv) It involves stealing money or other benefits by pretending to be someone else.

D) Credit Card Frauds

i) Purpose of credit card frauds is to obtain goods without paying

ii) To obtain unauthorized funds from account

iii) Credit card numbers are stolen from online databases.

6 DISCUSSION

All these crimes and motives behind them highlights unethical approach when compared with Ethics defined by Computer Ethics Institute. All these Ethics defined are defeated by these cyber crimes which clearly shows that Ethical approach while dealing in cyber space is missing.

1) Awareness program on 'Information Security' based on Cyber Ethics will help to prevent cyber crimes.
2) Protecting personal information while surfing online helps you to prevent from falling victim to cyber crime.
3) Cyber criminals may be amongst us who are copying the contents , taking ideas, writing and drawings intellectual property created by others from Internet and declaring/presenting as your own work. This is called Plagiarism which is an Ethical issue related to cyber crime.
4) Copying pirated softwares is also an Ethical issue related to cyber crime.
5) Set of rules on Internet called Netiquettes are missing in people. Implementation of Netiquettes is nothing but dealing ethically in cyber space.

Above discussion prove that if Ethical issues such as -- **Privacy, Information Security, Intellectual Property rights** are protected then there are less chances of falling victim to cyber crimes.

Therefore. this research paper strongly suggests that if Cyber Ethics are adapted by netizens of Maharashtra then chances of falling victim to cyber crimes at Individual and Organizational level will be less which will indirectly help in prevention and reduction of cyber crimes in Maharashtra.

7 REFERENCES

[1] Computer Ethics Institute- ten commandments from www.computerethicsinstitute.org/publications/tencommandments.html

[2] Cyber Crime Reports of 'National Crime Records Bureau of India' from 2009-2011

Cyber Crime reports (2009-11) from:

[3] Directorate of Forensic Laboratories, Santacruz, Mumbai

[4] Cyber crime Investigation Cell, Thane, Mumbai (India)

[5] Cyber crime Investigation Cell, Mumbai

[6] Cyber crime Investigation Cell, Pune

SAMPLE RTI APPLICATION FORM

To,
The Public information Officer
____
____
____
PIN: _______________________

Sir,

Subject: Request for Information under Right to Information Act 2005.

I Sri / Smt /Ms.
____
Son/Daughter/wife of Shri/Smt/Ms.
____
resident of
____,
telephone number (with STD Code)_____-______________________and/or mobile number:_______________________________wish to seek information as under

----

I hereby inform that following formalities have been completed by me:

1. That I have deposited the requisite fee of Rs.______/- by way of Cash / banker cheque / Draft / Postal Order/ others____________________) favoring
___________________________________dated_________________.

2. I need the photocopy of the documents and I had deposited the cost of the photocopy of Rs._____/- for______(Number of Pages)

or
3. I had deposited sum of Rs.______/- for the charges of CD. (strike out which ever is not applicable)

4. That I belong to Category of below Poverty Line (BPL): Yes / No
(Strike whichever is not applicable). If yes, I am attaching the valid photocopy of the certificate. Yes / No

5. That I am 'Citizen' of India and I am asking the information as 'Citizen'.

6. I assure that I shall not allow/ cause to use/ pass/share/display/ or circulate the information received in any case and under any circumstances, with any person or in any manner which would be detrimental to the Unity and Sovereignty or against the Interest of India.

Signature of the Applicant
Dated: