“A CRITICAL STUDY OF SECURITY MANAGEMENT SYSTEM OF CYBER CAFES IN PUNE CITY”

A Thesis Submitted to

Tilak Maharashtra Vidyapeeth, Pune

For the Degree of Doctor of Philosophy (Ph.D.)

In Management Subject

Under the Board of Management Studies

Submitted By

Mrs. Manisha M. Maddel

Under the Guidance of

Dr. Vilas Dattu Nandavadekar

November 2015

Declaration by the Candidate

I hereby declare that the thesis entitled **"A critical study of security management system of cyber cafes in Pune city"** completed and written by me has not previously formed the basis for the award of any Degree or other similar title upon me of this or any other University or examining body.

I further declare that the material obtained from other sources has been acknowledged in the thesis.

Mrs. Manisha M. Maddel

(Research Student)

Place: Pune

Date: 3 November 2015

Certificate of the Guide

This is to certify that the thesis entitled **“A critical study of security management system of cyber cafes in Pune city”** which is being submitted herewith for the award of the Degree of Philosophy (Ph.D.) under the faculty of Management of Tilak Maharashtra Vidyapeeth, Pune, is the result of original research work completed by Mrs. Manisha Mandar Maddel, 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 her.

Dr. Vilas Dattu Nandavadekar
(Research Guide)

Place: Pune

Date: 3 November 2015

Acknowledgement

I owe my personal thanks to **Prof. M.N. Navale** (Founder President, STES) and **Dr. (Mrs.) Sunanda Navale** (Founder Secretary, Sinhgad Institutes) for their whole hearted support, motivation and inspiring encouragement.

I am extremely grateful to my guide **Dr. Vilas D. Nandavadekar**, Director SIOM (MCA), Vadgaon (Bk.), Pune-41, for his encouragement and continuing support in this endeavour. His deep insights helped me at various stages of my research. Under his expert guidance I have completed my doctoral research on the topic "**A Critical Study of Security Management System of Cyber Cafes in Pune City**".

Very special thanks to **Dr. Deepak J. Tilak** (Vice-Chancellor, Tilak Maharashtra Vidyapeeth, Pune) and **Dr. Umesh Keskar** (Registrar, Tilak Maharashtra Vidyapeeth, Pune) for giving me the opportunity to carry out my doctoral research.

My sincere gratitude and heartfelt thanks is reserved for **Dr. Manisha Kumbhar, Dr. Vidya Gavekar and Dr. Shivaji D. Mundhe** for their timely guidance and valuable inputs. A big "Thank you!" also goes out to all Cyber cafe Owners and Visitors who helped me by giving the required information.

Finally, I would like to acknowledge the most important people in my life my husband Mr. **Mandar Maddel,** my parents **Mr. Arun Khandode** and **Mrs. Radha Khandode,** my in-laws **Mr. Dattatraya Maddel** and **Mrs. Shakuntala Maddel** & my son **Arya** for their extraordinary support, love patience and understanding throughout my long journey. Their support and tolerance has proved great help in the fulfillment of this mammoth task.

Mrs. Manisha M. Maddel

CONTENTS

I. List of Tables and Graphs

II. List of Figures

III. List of Maps

IV. List of Annexures

V. Publications by Researcher

Sr. No	Paper Title	Publication
1	Enhancing Social Security through Cyber Security for Cyber Cafe	Pezzottaite Journals International Journal of Information Technology and Computer Sciences Perspectives Volume – 3 Number -4 ,October – December – 2014 ISSN(P): 2319-9016 , ISSN(O): 2319-9024 IF-2012: 3.201, IF-2013: 5.058
2	Wireless Security – Cyber Cafe Wi-Fi Security Awareness	International Conference Proceedings "Globe Unified : Role of ICT - 2015" (GURICT -2015) 12th to 14th Feb-2015 ISBN – 978-81-910118-9-0
3	Ramification of Wireless Fidelity "Wi-Fi": New Challenges for Wi-Fi security.	National Conference Proceeding "Recent Trends in computer science and applications and computational mathematics (RTCSACM-2012) 21ST to 22nd December 2012 ISBN: 978-93-5097-319-6
4	Implications of Cyber Crime through Cyber Cafe and Suggestive Measure to prevent Cyber Crime	International Journal of computer application and management (IJCAAM) ISSN No. :2231-6957 Volume -I Issue -1,July - 2011

Workshop Attended by Researcher

Sr. No	Workshop Attended	Conducted By
1.	Two week ISTE Cyber Security workshop	Symbiosis Institute of Computer Studies and Research (SICSR) , Indian Institute of Technology (IIT) Bombay from 10th July -20th July 2014
2	National Level Two Days Workshop on Cyber Security'	IMSCDR, Sponsored by BCUD, Savitribai Phule Pune University' 18th and 19th December, 2014

Glossary of Item

Term	Definition
Access Control	Access Control ensures that resources are only granted to those users who are entitled to them.
Auditing	Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.
Authentication	Authentication is the process of confirming the correctness of the claimed identity.
Authenticity	Authenticity is the validity and conformance of the original information.
Authorization	Authorization is the approval, permission, or empowerment for someone or something to do something.
Availability	Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it
Access Point	A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network
Accountability	Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information
Ad Hoc Network	A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. Government - approved cryptographic algorithm that can be used to protect Electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.
Anomaly - Based Detection	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
Anti -jam	Countermeasures ensuring that transmitted information can be received despite deliberate jamming attempts
Anti-spoof	Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker
Antispyware Software	A program that specializes in detecting both malware and non - Malware forms of spyware.
Antivirus Software	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents

Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges
Availability	Ensuring timely and reliable access to and use of information
Back Door	Typically unauthorized hidden software or hardware mechanism used to circumvent security controls
Biometrics	Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics
Boot Record Infector	A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.
Botnet	A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them
Computer Emergency Response Team (CERT)	An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publishes alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.
Confidentiality	Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.
Cost Benefit	A cost benefit analysis compares the cost of implementing

Analysis	countermeasures with the value of the reduced risk.
Computer Incident Response Team – (CIRT)	Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team)
Comp uter Security	Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Content Filtering	The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.
Cyber Infrastructure	Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer Systems, and embedded processors and controllers.

Data Encryption Standard (DES)	Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46.
Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit
Data Loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time - critical operations. (Time - critical may be milliseconds or it may be hours, depending upon the service provided.)
Distributed Denial of Service	A Denial of Service technique that uses numerous hosts to perform the attack
Eavesdropping Attack	An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system
Encryption	Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents , or data transmissions, or to establish or exchange a session key for these same purposes.
Firewall	A gateway that limits access between networks in accordance with local security policy. A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.
Firewall Control Proxy	The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination
Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution
Forensics	The practice of gathering, retaining, and analyzing computer-related

	data for investigative purposes in a manner that maintains the integrity of the data.
Gateway	Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
Hacker	Unauthorized user who attempts to or gains access to an information system.
Hardware	The physical components of an information system. See also Software and Firmware.
Honeypot	A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Inside(r) Threat	An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internet Protocol (IP)	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Intranet	A private network that is employed within the confines of a given enterprise
Intrusion	Unauthorized act of bypassing the security mechanisms of a system.
Intrusion Detection Systems (IDS)	Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
Intrusion prevention System(s) (IPS)	System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Key Logger	A program designed to record which keys are pressed on a computer

	keyboard used to obtain passwords or encryption keys and thus bypass other security measures.
Logic Bomb	A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
Malicious Logic	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
Man-in-the-middle Attack – (MitM)	An attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.
Mandatory Access Control (MAC)	A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity.
Masquerading	When an unauthorized agent claims the identity of another agent, it is said to be masquerading.
Metrics	Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
Network Sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Non-repudiation	Assurance that the sender of information is provided with proof of

	delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Operations Security (OPSEC)	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.
Packet Filter	A routing device that provides access control functionality for host addresses and communication sessions.
Packet Sniffer	Software that observes and records network traffic.
Passive Attack	An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping).
Passive Wiretapping	The monitoring or recording of data while it is being transmitted over a communications link, without altering or affecting the data.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Privilege	A right granted to an individual, a program, or a process
Profiling	Measuring the characteristics of expected activity so that changes to

	it can be more easily identified.
Protocol	Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.
Proxy	A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email.
Proxy Server	A server that services the requests of its clients by forwarding those requests to other servers.
Radio Frequency Identification – (RFID)	A form of automatic identification and data capture (AIDC) that uses electric or magnetic fields at radio frequencies to transmit information.
Remote Access	Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).
Repository	A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurs.
Risk Analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system.
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational

	assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Risk Response Measure	A specific action taken to respond to an identified risk.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Robustness	The ability of an Information Assurance entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.
Rogue Device	An unauthorized node on a network.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spam Filtering Software	A program that analyzes emails to look for characteristics of spam, and typically places messages that appear to be spam in a separate email folder.
Spoofing	“IP spoofing” refers to sending a network packet that appears to come from a source other than its actual source.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Tampering	An intentional event resulting in modification of a system, its intended behavior, or data.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Threat Assessment	Formal description and evaluation of threat to an information system.
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact.
Threat Monitoring	Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.
Time Bomb	Resident computer program that triggers an unauthorized act at a predefined time.
Trap Door	A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data.

Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Unauthorized Access	Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks, which provides a secure communications tunnel for data and other information transmitted between networks.
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread it to other computers, or even erase everything on a hard disk.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Wi-Fi Protected Access-2 (WPA2)	The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard.
Wired Equivalent Privacy (WEP)	A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.
Wireless Access Point (WAP)	A device that acts as a conduit to connect wireless communication devices together to allow them to communicate and create a wireless network.
Wireless Application Protocol – (WAP)	A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.
Wireless Technology	Technology that permits the transfer of information between separated points without physical connection.
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

*Sources: csrc.**nist**.gov/publications/drafts/ir-**7298**-rev2/**nistir7298**_r2_draft.pdf*

CHAPTER 1

INTRODUCTION

"Any successful organization needs to advance in all three domains of people, process and technology. But it starts with good people to advance the latter."

Rich Mason, Honeywell

1.1. Introduction

Information Technology has grown tremendously during the last two decades and became the main source of knowledge. The latest information and the current technology [4] make information available through Internet. Information through internet is useful for novice and also to the expert in all fields of knowledge. Information Communication Technologies (ICT) is the main model of use for using public Internet facilities in order to access information. In developing countries public [5] and shared facilities help to create desperately needed access for information sharing and information access. In the context of public access, Cyber Cafes play an important role as the most common Internet access model. Cyber Cafe are one of the major public access to ICT and have been contributing a lot in the internet penetration and to reduce the digital divide in India and all around the world[22].

Although Internet is a vital source of information, the Cyber-crime has also increased. The Owners of Internet cafes extend the freedom of use of Internet access to the community but they fail to tighten their computer security to safeguard the private information of their Visitors. Cyber security management plays a vital role for Cyber Cafe Owners and Visitors. Every day new threats and cyber-attacks are created and taking place. Internet and computer used for it are becoming tools for cyber-crime. Attacks by cyber criminals can be potentially just as damaging to the national infrastructure as attacks by terrorists. The remarkable growth of Cyber Cafe and Internet access has created the problem of Cyber-crime propagation with lack of strong evidence resulting in investigation difficulties. These cyber threats arises due to vulnerabilities ,lack of cyber security awareness and lack of cyber security preventive measures taken while using the internet cafe. These cyber security risk need to be handled by identifying threats and vulnerability and the impacts of these threats. Existing laws for Cyber-crime are not up to the mark since technology changes at a faster rate and every time new type of Cyber-crime takes place. The preventive measures taken by internet users are not effective to avoid Cyber-crime. Due to the gap between faster occurring of Cyber-crimes and slow changes in the amendment of law. There is a strong need of legal protection from government side to protect businesses. These protections will have to adopt technical measures to protect businesses from those who would steal, denies access to, or destroys valuable information. Defense mechanism against cyber attacks should be dynamic and strong enough. Cyber Cafe along with other public internet access point can be cyber safe if proper cyber security management is considered and implemented.

1.2. Globalization & Revolution in Information Communication Technology

Information Communication Technology (ICT) is a major factor in the international integration arising from exchange of things and ideas. It forms a driving factor for globalization. Technology is growing at a tremendous rate, new hardware, software and networks are improving day by day which helps in communicating at a faster rate resulting in growth of economy in all sectors. Global integration is a result of exchange of ideas, product, views and resources among different nations for which communication among people has to be faster. Advancement in ICT has provided the path for international globalization regardless of the geographic location.

ICT revolution is termed as to process information in digital form and communicate it. ICT revolution has improved the lives of many people in the society. Society as whole is improving in terms of standards and improved life style with economic growth. Communication by making use of ICT is done through various ways such as emails, chatrooms, and websites, messaging systems such as WhatsApp, Hike messenger etc. which has brought people together of same interest to achieve their goals and improve their business. Businesses are flourishing due to ICT since decision making is becoming faster as the analysis of information is done in less time span. Also there is fair competition between businesses avoiding monopoly of few companies. Literacy rate is also growing high due to reach of ICT in rural and urban areas. More number of jobs is created which has improved the living standards of the people. ICT revolution has helped in education sector by way of demonstrating the world facts and making the world to come closer. This is possible through internet, Software, online educational material and chat application.

ICT revolution helps in globalization but there is other darker side for it as well. Though the faster changing technology is helping mankind to improve and grow by all means and in all sectors, it is also used by attackers or sick minded people for illicit purposes. The lacuna in rules and regulations and difficulties in investigating the Cyber-crime has added one more helping hand for such criminals. ICT should be used for betterment of society and protected from unlawful deeds.

1.2.1. Cyber Space Usage: World and Indian Scenario

Internet forms prime component of cyber space. It provides an environment for communication and exchange of information and resources. Using this environment people with illicit purpose can create false identity to hide real identity and cheat other people on the network. Cyber security awareness, protecting the network infrastructure along with suitable measures to avoid Cyber-crime is an important aspect that needs to be considered. According to Department of Electronics and Information Technology, internet is a powerful tool that should be used for betterment of society and growth of economy. Internet is a key component of national infrastructure. Table No.1.1 shows a comparative Usage of cyber space World wide and in India during the years 2005 – 2012. India stands in top five Countries in web hosting.

Table No. 1.1: A Comparative Usage of Cyber Space Worldwide and in India during the years 2005 and 2012

Cyber Space Usage	World Wide		India	
	2005	2012	2005	2012
Total Number of Websites	7.5 million	698 million (registered) 209 million(active)	1.7 Lakhs	1.4 million 1.7 million '.in'(registered) 1 million '.in'(active)
Number of Internet Users	720 million	2.41 billion	21 million	150 million
Number of email accounts	315 million	3.146 billion	11 million	180 million

Sources: Standing committee on Information technology (2013-14) - Cyber-crime, cyber security and right to privacy: fifty-Second Report [2]

Most of the internet users use internet without understanding the dangers associated with it. As per the technological changes the internet users need to update themselves frequently. Along with individual responsibility the government needs to take efforts for cyber security management and protecting the cyber space. In today's scenario the major factors for Cyber-crime and threats are lack of awareness, lacunas on technological aspects, poor management of cyber security, and lack of cyber security knowledge and careless attitude.

1.2.2. ICT Initiatives in Smart Cities

Smart Cities are new concepts that are emerging all over the world. IBM started with the concept of smart city in their project Smarter Planet Initiative in 2008 and slowly all nation started thinking on the same line. Most of the developed nations started research for smart cities and invested heavily on it. Numbers of example are now ready for smart cities such as countries like UAE, South Korea Málaga, Malta Amsterdam, Cairo and Lyon.

ICT plays an important part for implementation of smart cities. Smart cities make use of different technologies such as Wi-Fi, sensor technology, anywhere any time communication, and intelligent systems to take care of the services required and to solve the problems. It also continuously works on future scope and challenges for new and exciting smart city features. This requires on spot collection of data, analyzing the data, identifying the threats and vulnerabilities and risk associated with it along with proper risk management to be done. Some of the highlighting features of the smart cities include routing the traffic automatically without jamming, avoiding accidents, detection of Cyber-crimes at a faster rate, identifying a place to park the vehicle, showing locations to users such as hotspot, hotels, airports etc. Many services such as help for elderly on a click of button, medical care, and commerce can be improved and education in a more understandable manner can be given to students. The best part of it is smart city can keep transparency among society and government. It will enable citizens to understand government policies and also they can provide suggestions on certain issues quickly while interacting with government officials.[23]

With smart cities services, citizens make use of Wi-Fi at internet cafes or portals in shopping malls or in government buildings for exchange of information or transactions. Kiosk or Internet Cafe, Wired or Wireless is used for information search and guidance and playing online games in smart cities. Smart cities are the potential future for every Nation.

However growth of smart cities and ICT complexity will also lead to increasing vulnerability, which may have malicious attacks and unintentional incidents. Security threats are integral thoughts during smart cities planning.

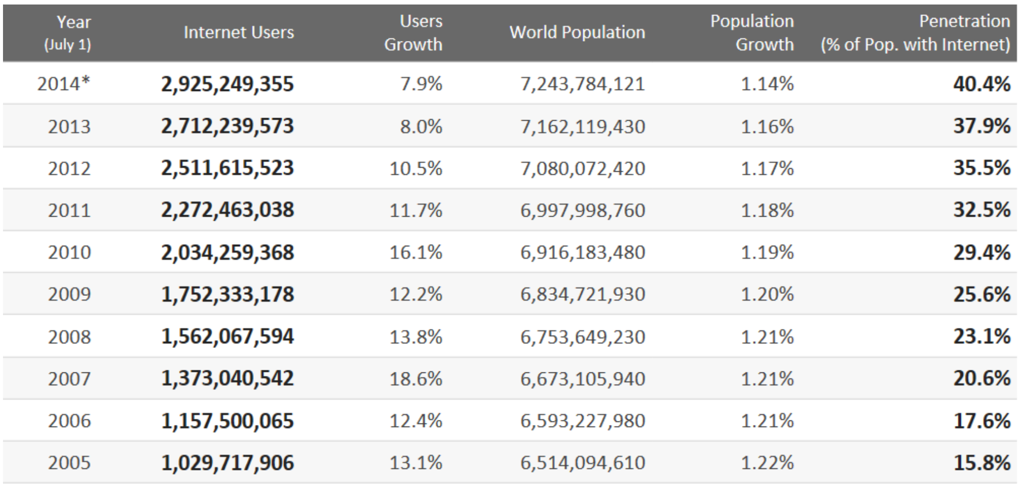
1.3. Internet and its Users

Internet today is a driving force in the world in which everything is e-enabled. The internet is a powerful medium for ICT and it empowers governments to extend their services more effectively to the people. Public Internet Access point were started with the objectives that include better use of information, better education, communication, economic and social growth. [18] Cyber Cafe provides its main service as the internet service for a fee. The internet is used for various purposes such as electronic mail, entertainment, research, searching of information, availing various government services, advertising, social networking, online services for product purchase or sell etc. [17] it has become the very important factor of people in the society.

1.3.1 History of Internet

The internet is changing and it will continue to do so. The number of internet users is increasing day by day. Table No.1.2 (A) shows the growth of internet users in the world from 2005-2014. Around 40% of the world population has an internet connection today. The number of internet users has increased to a greater extent from 1999 to 2013. The first billion was reached in 2005. The second billion of internet users reached in 2010 and third billion in 2014. It is observed that Internet users have grown to 2,925,249,355 in the year 2014. The chart and table below show the number of global internet users per year since 2005:

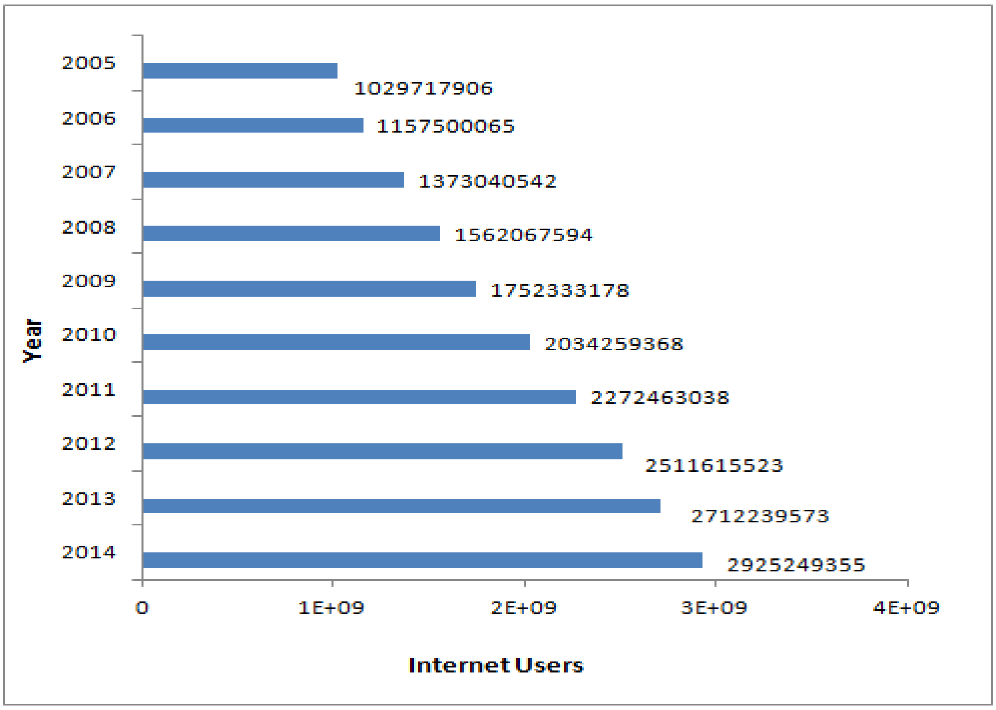
Table No.1.2 (A): The Growth of Internet Users in the World from 2005-2014



Year (July 1)	Internet Users	Users Growth	World Population	Population Growth	Penetration (% of Pop. with Internet)
2014*	**2,925,249,355**	7.9%	7,243,784,121	1.14%	**40.4%**
2013	**2,712,239,573**	8.0%	7,162,119,430	1.16%	**37.9%**
2012	**2,511,615,523**	10.5%	7,080,072,420	1.17%	**35.5%**
2011	**2,272,463,038**	11.7%	6,997,998,760	1.18%	**32.5%**
2010	**2,034,259,368**	16.1%	6,916,183,480	1.19%	**29.4%**
2009	**1,752,333,178**	12.2%	6,834,721,930	1.20%	**25.6%**
2008	**1,562,067,594**	13.8%	6,753,649,230	1.21%	**23.1%**
2007	**1,373,040,542**	18.6%	6,673,105,940	1.21%	**20.6%**
2006	**1,157,500,065**	12.4%	6,593,227,980	1.21%	**17.6%**
2005	**1,029,717,906**	13.1%	6,514,094,610	1.22%	**15.8%**

Sources: Internetlivestats.com/internet-users [16]

Graph No.1.1: Growth of Internet Users in the World from 2005-2014



Sources: Internetlivestats.com/internet-user/[16]

Table No.1.2 (B) shows the growth of internet users in the different countries. The statistics reveals that china has the largest number of internet users i.e. 641,601,070, million United States is at second position 279,834,232 million and India stands at third position with 243,198,922 million number of internet users. There is 14% growth rate of internet users in India.

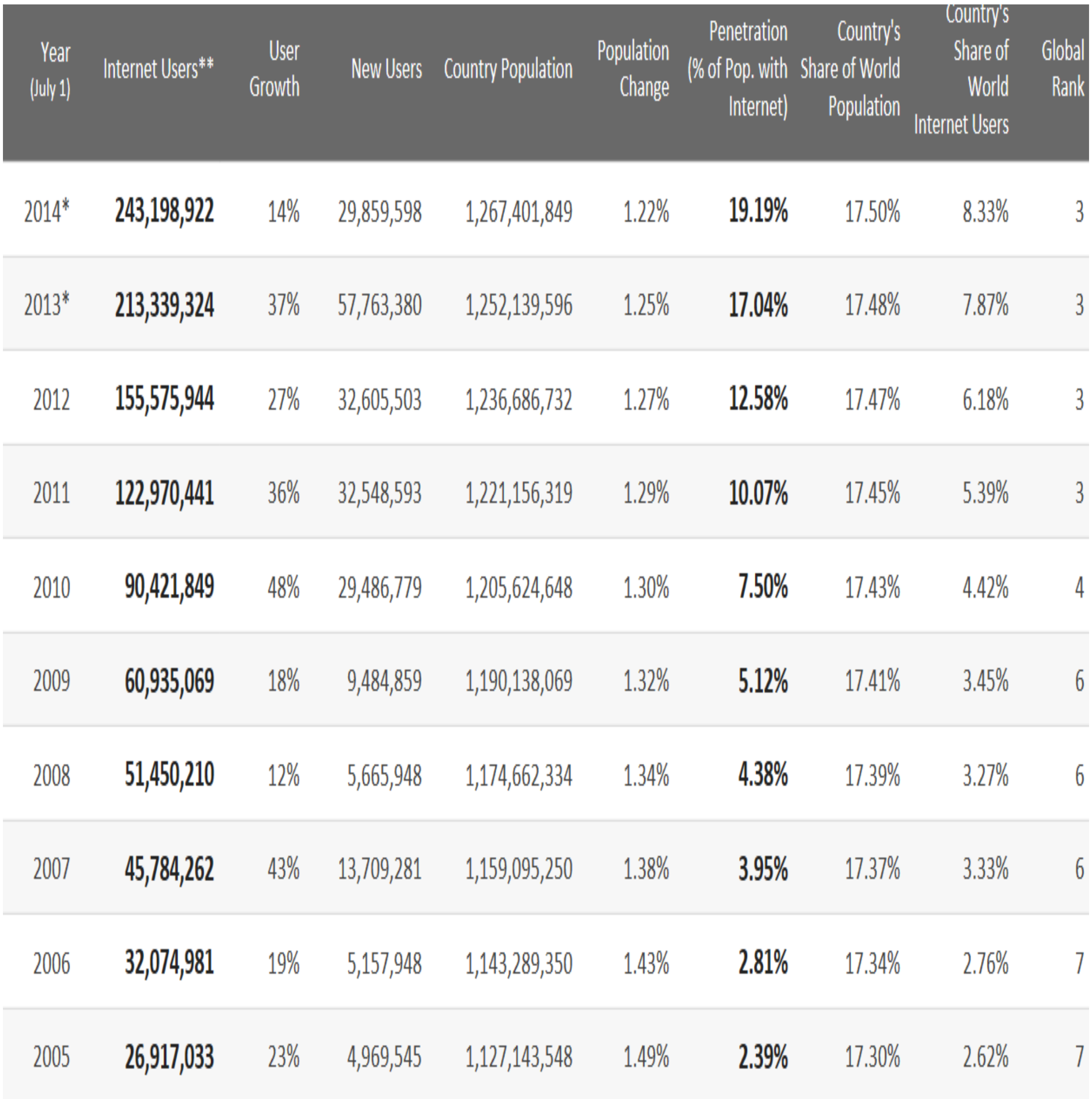
Table No.1.2 (B): List of Countries by Growth Percentage of Internet Users

Rank	Country	Internet Users	1 Year Growth Percentage
1	China	641,601,070	4
2	United States	279,834,232	7
3	India	243,198,922	14
4	Japan	109,252,912	8
5	Brazil	107,822,831	7
6	Russia	84,437,793	10
7	Germany	71,727,551	2
8	Nigeria	67,101,452	16
9	United Kingdom	57,075,826	3
10	France	55,429,382	3

1.3.2 Internet users in India

Population of India is 1,267,401,849 billion in 27 states, 7 union territories and it is the world's largest English speaking nation. India's internet population is growing at a fast pace. In India people are know the importance of the internet in their lives where they perform various task like learning [16], searching social networking, shopping, gaming, banking chatting etc. Public access point like Cyber Cafe helps people to make use of internet services for these purposes. It is observed from the Table. No 1.2 & 1.3 that in the year 2014, India stands at third global rank with 241,198,922 internet users and as compared to year 2013 there is 14% growth in internet users. Graph No. 1.2 shows the growth of Internet users in India from 2005-2014.

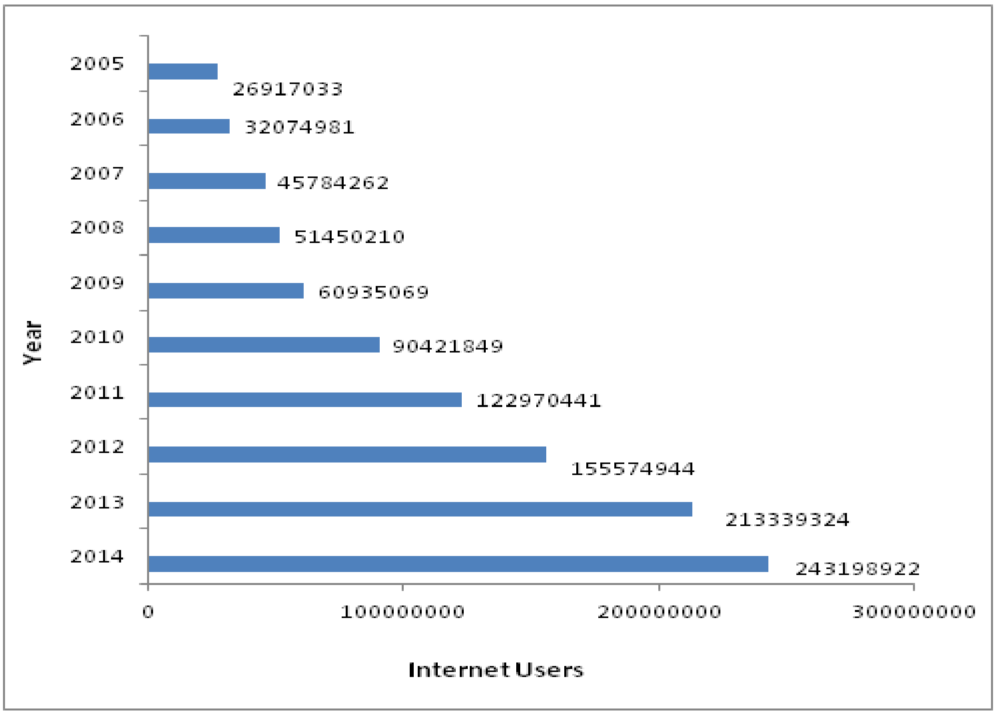
Table No.1.3: Growth of Internet Users in India from 2005-2014



Year (July 1)	Internet Users**	User Growth	New Users	Country Population	Population Change	Penetration (% of Pop. with Internet)	Country's Share of World Population	Country's Share of World Internet Users	Global Rank
2014*	**243,198,922**	14%	29,859,598	1,267,401,849	1.22%	**19.19%**	17.50%	8.33%	3
2013*	**213,339,324**	37%	57,763,380	1,252,139,596	1.25%	**17.04%**	17.48%	7.87%	3
2012	**155,575,944**	27%	32,605,503	1,236,686,732	1.27%	**12.58%**	17.47%	6.18%	3
2011	**122,970,441**	36%	32,548,593	1,221,156,319	1.29%	**10.07%**	17.45%	5.39%	3
2010	**90,421,849**	48%	29,486,779	1,205,624,648	1.30%	**7.50%**	17.43%	4.42%	4
2009	**60,935,069**	18%	9,484,859	1,190,138,069	1.32%	**5.12%**	17.41%	3.45%	6
2008	**51,450,210**	12%	5,665,948	1,174,662,334	1.34%	**4.38%**	17.39%	3.27%	6
2007	**45,784,262**	43%	13,709,281	1,159,095,250	1.38%	**3.95%**	17.37%	3.33%	6
2006	**32,074,981**	19%	5,157,948	1,143,289,350	1.43%	**2.81%**	17.34%	2.76%	7
2005	**26,917,033**	23%	4,969,545	1,127,143,548	1.49%	**2.39%**	17.30%	2.62%	7

Sources: Internetlivestats.com/internet-users/ [16]

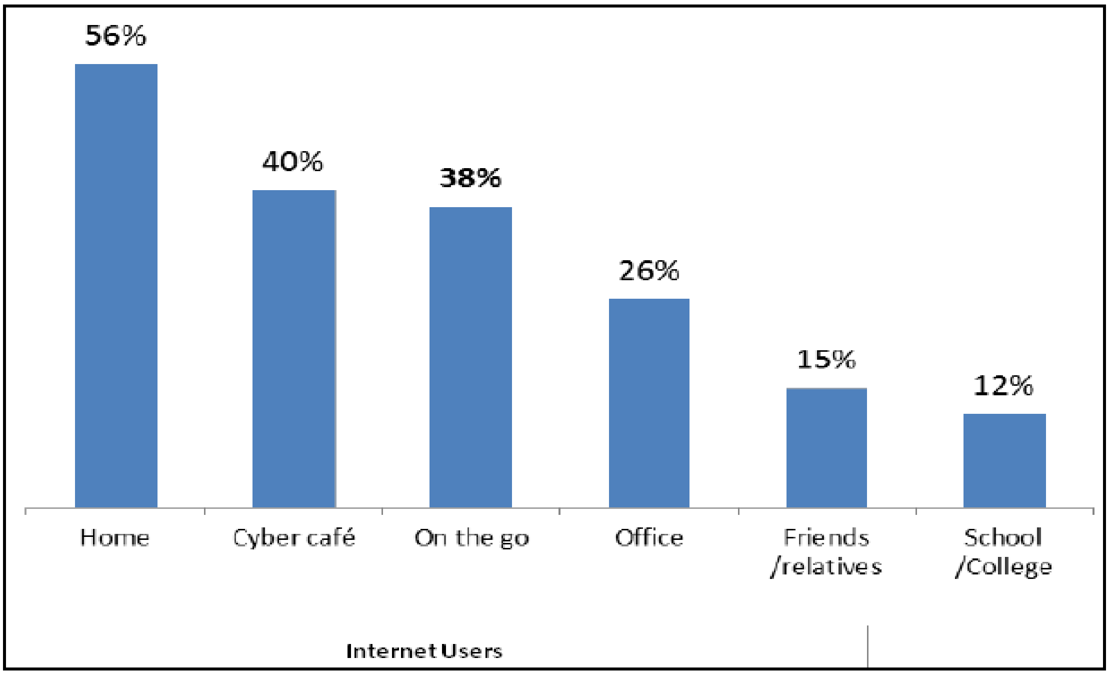
Graph No.1.2: Growth of Internet Users in India from 2005-2014



1.3.3 Points of Internet Access in India

Major point of internet access for most of Indian citizens is their home forming 56 percent of population. From the Graph-1.3 it is seen that Cyber Cafes are the main point of access with 40 percent of them making use of Cyber Cafe. This is mainly because of the availability of sufficient infrastructure. Due to mobility offered by mobile phones and tablets they are increasingly becoming the point of internet access forming 38 percent of them. 26 percent make use of office as internet access point. [15] 15 percent make use of friends and relatives places to access the internet and 12 percent make use of schools to access internet. Thus it can be seen that majority of people access internet through Cyber Cafe.

Graph No.1.3: Internet Access Point in Urban Indian



Sources: IMRB I-Cube June 2013[15]

1.3.4 Public Internet Access Point

Public Internet Access Point (PIAP) is public place where people access internet services. For computer and internet access and internet services, millions of people around the world depend on public access points like libraries, tele centers, and kiosk or Cyber Cafes. Most of these public access points are commercial venues like internet cafe and other types such as library are seen. In rural areas tele centers and Cyber Cafe are seen and are supported by government and development agencies with the intention that having internet and computer knowledge will help in development of the nation and world. Cyber Cafe is a place which provides Internet access to the public usually for a fee.[24] Cyber Cafes models are most used in urban areas for public internet access other than other public facilities like libraries, institutes, organizations, schools colleges or universities. Internet cafe model is shared access model which is less expensive as compared to the personal owned models which require cost of hardware, software and maintenance. These businesses usually provide snacks and drinks, hence the word cafe is associated with in the name [14]. The fee for using a computer is usually charged at a time-based rate.

1.4 Cyber Cafe Preliminaries

An Internet cafe or Cyber Cafe is a place which provides internet access to the public, usually for a fee. It includes any commercial establishment or Internet kiosk, the objective of which is to make Internet services available to the general public .The fee for using a computer is usually charged as a time-based rate. Cyber Cafe is considered to be a "Place of Public Amusement "as defined under section 2 (9) of the Bombay Police Act, 1951" (Act XXII of 1951).[25]Cyber Cafe license is allotted only after checking if all norms provided by the government are fulfilled.

The first online cafe in South Korea called Electronic Café was started near Hongik University by Ahn Sang-Su and Keum Nuri in Seoulin [14]March 1988. In this cafe telephone lines were connected to two 16 bit computers for internet services. VSNL introduces internet in India via dial up connection in 6 cities on August 2014.

India's first Cyber Cafe was opened in Mumbai by Pritish Nandy in 1996 at Hotel Leela Kempinski. In 1998 India introduced new internet policy and Sify was first ISP. Internet cafes are the primary form of Internet access for people as a shared-access model which is more affordable than personal ownership of computer system and internet connections. LAN gaming center was also one of the Cyber Cafe model where various players play game online. These players can be connected to various other players in some different locations. These Cyber Cafes provide multiplayer games which are popular. Gaming Cyber Cafe have a large demand various countries by youth and children's and thus have become a popular model for earning profit.

To sustain in this competitive world Cyber Cafe Owners have started attracting the Visitors by various means such as low price for fee, more hours of access, good quality of hardware and selling computer accessories ,selling food, beverages, telephone cards to its Visitors. Although Cyber Cafe are famous and useful model for internet access along with it comes the responsibility. In India there are many rural areas who still cannot afford to invest in computers hardware and software to access internet, in such area Cyber Cafe can be of great help as e-learning hubs. It will be beneficial that Cyber Cafes can be considered as an fundamental part of the e-governance schemes.

1.4.1 Internet Cafes in Developing World and its Significance

Internet cafes in the world are declining as the growth of smartphones are increasing. Smartphones helps in anywhere and anytime internet facility. In July 2013 a five year study released by the university of Washington states that in developing countries Cyber Cafe still remains as model of internet access. Prof. Chris Coward of the university stated that “One Technology doesn’t replace the other” [7] and thus Cyber Cafe will still stay as internet access venue even though smartphones are available.

Mobile phones “will not solve the access problem.” Internet cafe provides economically backward people to access internet service. These Cyber Cafe [7] provide internet service at low cost, good speed, and other facilities. Most of the internet users at Cyber Cafe come for information sharing through email, chatting or instant messaging software’s and websites. Internet cafe operators also provide help to the Visitors who are inexperienced and have less knowledge of computers and internet. Also Cyber Cafe works as a venue for support, learning, research and education along with learning new tools to overcome the problem of not having sufficient skills to use internet for information exchange.

In India Cyber Cafes are used for the purpose of development, entertainment as well as for commerce. For some individuals it is the only source for computer and internet access. Cyber Cafes are also useful for some individuals as compared to home since it provides good speed and good hardware. For some people it provides a an warm environment for social networking. Cyber Cafe can boost individual curiosity and help novice users to develop, learn and improve digital skills. For some

Visitors it also provides operator assistance in case they are not able to understand how to use some of internet services especially for elderly people. If Cyber Cafes or public internet access venues are not there then usage of ICT would definitely decline. Cyber Cafe bridges the gap between technical people and people with no knowledge of ICT. It helps to fill the communication gap, improves social cohesion and keeps the world connected. It may take decades for some countries to reach high levels and quality of home connectivity, thus, public ICT access like Cyber Cafe will remain an important service.[21]

1.4.2 Cyber Cafe Stakeholders:

Cyber Cafe stakeholders are the Owners who are responsible for the Cyber Cafe, its services and activities, Visitors using the Cyber Cafe services and government official involved in monitoring the activities of the Cyber Cafe. The Owners play a vital role in the effective operationalization of Cyber Cafe. He is responsible for all the activities in Cyber Cafe along with its cyber security management. Owners follow the rules and regulations set by the government for Cyber Cafe security. He keeps himself updated with latest security techniques and procedures and Cyber-crime law. Visitors are the people who visit Cyber Cafe to use its service like internet access, printing scanning, etc. Visitors visiting the Cyber Cafe should be aware about cyber security and Cyber-crime to avoid Cyber-crime attack. Government official are people who monitor the Cyber Cafe, its activities, take audit at regular intervals and check whether government norms are followed by the Cyber Cafe Owners.

1.4.3 Social and Economic Impact of Cyber Cafe to ICT

Public access point like Cyber Cafe has a variety of impacts on ICT. Digital inclusion is the fundamental effect and the other is social and economic impact. It is very clear that people lacking access to ICTs will affect the economy of the country. Cyber Cafe helps people to overcome limitations such as lack of technological skills or poverty which affect the use of ICT and in turn affecting the economy. From the perspective of users, using computers and the internet at public access venues provides benefit in multiple aspects in their lives which include Education, Employment & Income, research, Government work, and Communications Culture improvement by blog and websites, Travel & Entertainment. Thus it is very clear that public access point such as Cyber Cafe affects the nations and even individual lives in terms of personal growth, economic growth and social wellbeing.

1.4.4 Present Status of Cyber Cafe in Pune:

Pune is an educational hub with lot of young students studying in different fields. Pune was called "The Oxford of the East" by Jawaharlal Nehru India's first Prime Minister, due to the well-known academic and research institutions in the city. [28] There is growing need for internet connection. This gave rise to increase in Cyber Cafe for internet services. Also due to IT hub people are more aware about security and make use of Cyber Cafe for various purposes such as research, commercial purpose, e-governance services etc. Today there are 259 registered Cyber Cafes in Pune city along with many unregistered Cyber Cafe. Most of Cyber Cafe offers internet service to Visitors in terms of broadband service and Broadband Wi-Fi.

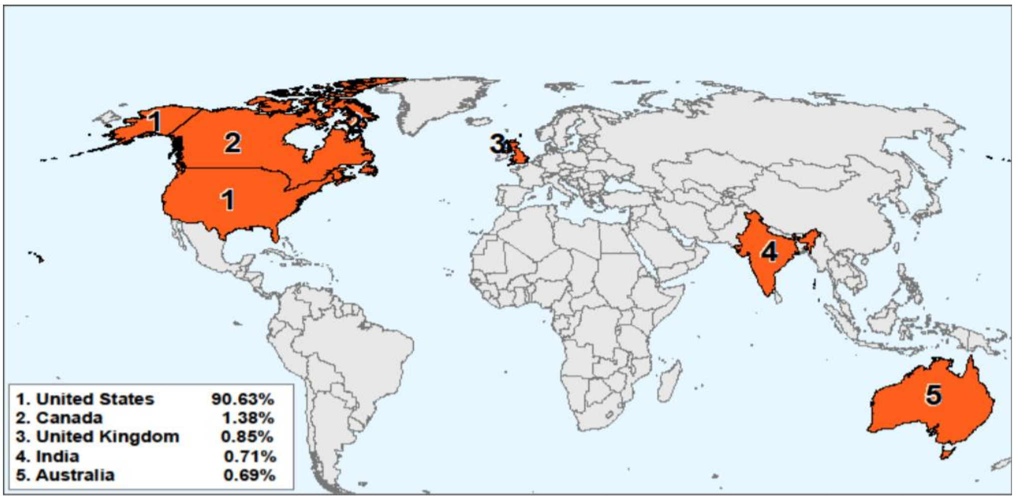
1.5 Cyber Crime and its Escalation

Cyber-crime is a term in which criminal activities are done using the medium of computers or computer networks. Thus internet, cyber space and the worldwide web can be used to commit crime. [13]The evolution of internet and the revolution of crime start together. The cyber criminals commit acts of crime and illicit act on the World Wide Web. Internet crime takes numerous forms such as Hacking, Phishing, Cyber Vandalism, Spamming, Spoofing, DoS, Backdoor, and Trojan etc. harming many people by harassing them, stealing or tampering their data, causing harm to the information infrastructure, robbing money by gaining their bank credentials and many more .

1.5.1 Growth of Cyber Crime

The Map 1.1 shows the top five countries ranked by the number of victim complaints reported to the IC3 during 2013. From the Map it can be seen that India ranks fourth in cyber complaints registered. United States stand first followed by Canada and on third positon United Kingdom. Australia ranks fifth in Cyber-crime complaints registration. Cyber Criminals make use of different types of techniques to make scams to cheat Internet users. These frauds are of various types such as identity theft, lottery scam, Nigerian fraud or hacking and malicious software or malware scams. Some recurring and common crime schemes include Ransomware/Scareware Scams, Child Pornography Scareware, Fake or Rogue Anti-Virus Software, Real-Estate Rental Scams, Work-at-Home (Employment) Scams, Identity Theft, Credit Card Fraud, Lotteries, Phishing and Spoofing.

Map No.1.1: Top Five countries Ranked by the Total Number of Complaints Received by IC3 in 2013



Sources: ic3.gov [13]

1.5.2 Cyber Crime in India:

The Nation Crime Records Bureau (NCRB), Ministry of Home Affairs has shown Cyber-crime Statistics for the year 2013, which clearly reflect that there is rapid increase in Cyber-crime by 50 percent on year to year basis from 2012 to 2013. India stands fourth in the world for Cyber-crime. In the year 2013 a total of 5693 cases were registered under different Cyber-crime offences and a total of 3301 people were arrested. Table No. 1.5 shows that maximum offenders came from the 18-30 age groups. Among states, the highest incidents of Cyber-crime took place in Maharashtra (681(IT Act)) followed by Andhra Pradesh (635(IT Act)) and Karnataka (513(IT Act)).Table No.1.4 shows the details of registered Cases and Persons [19] arrested under Cyber-crime in India.

Table No.1.4: Incidence of Cases Registered and Number of Persons Arrested Under Cyber Crimes (IT Act + IPC Sections) During 2013 (All-India)

Sr. No.	Crime Head	Cases Registered	Persons Arrested
	A. Offences under IT Act		
1	Tampering computer source documents	137	59
2	Hacking with computer system		
	i) Loss/Damage to computer Resource/Utility	1966	818
	ii)Hacking	550	193
3	Obscene Publications/Transmission in electronic form	1203	737
4	Failure		
	i) Of compliance/orders of Certifying Authority	13	3
	ii)To assist in decrypting the information intercepted by Govt. agency	6	7
5	Un-Authorized access/attempt to access of protected computer system	27	17
6	Obtaining license or Digital Signature Certificate by misrepresentation/suppression of fact	12	14
7	Publishing false Digital Signature Certificate	4	8
8	Fraud Digital Signature Certificate	71	51
9	Breach of confidentiality/privacy	93	30
10	Other	274	161
11	Total (A)	4356	2098
	B. Offences under IPC		
1	Offences by/against public servant	1	2
2	False electronic evidence	6	7
3	Destruction of electronic evidence	6	4
4	Forgery	747	626
5	Criminal Breach of trust fraud	518	471
6	Counterfeiting		
	i)Property/mark	10	34
	ii)Tampering	8	10
	iii)Currency/stamps	41	49
7	Total (B)	1337	1203
	Grand Total (A+B)	5693	3301

Sources: ncrb.gov.in[19]

1.5.3 Present Status of Cyber Crime in Maharashtra

Cyber-crime in Maharashtra is growing very fast. As per a recent Criminal Investigation Department(CID) Maharashtra 2013 report on crimes in the state, the intention behind crimes can be revenge, money, harassing individual for fun or jealousy, desire to disrepute someone or may be eve teasing. The report said that Cyber-crimes suspects in many cases were business competitors, foreign nationals or groups, unhappy employees, hackers, students or professional learners, neighbors, relatives or friends of victims. Maximum Cyber-crime occurs due to lack of awareness about Cyber-crime and cyber security.

TableNo.1.5: Incidences of Cases Registered Under Cyber-crimes in States/UTs during 2012 & 2013 and Percentage Variation

Sr. No.	**State/UT**	**IT Act**			**IPC Section**		
		2012	**2013**	**% Variation**	**2012**	**2013**	**% Variation**
STATES:							
1	ANDHRA PRADESH	429	635	48.0	25	16	-36.0
2	ARUNACHAL PRADESH	12	10	-16.7	0	0	@
3	ASSAM	28	154	450.0	0	0	@
4	BIHAR	23	23	0.0	7	116	1557.1
5	CHHATTISGARH	49	91	85.7	10	10	0.0
6	GOA	30	57	90.0	2	1	-50.0
7	GUJRAT	68	61	-10.3	10	16	60.0
8	HARYANA	66	112	69.7	116	211	81.9
9	HIMACHAL PRADESH	20	24	20.2	0	4	@
10	JAMMU AND KASHMIR	35	46	31.4	0	0	@
11	JHARKHAND	10	13	30.0	25	13	-48.0
12	KARNATAKA	412	513	24.5	25	20	-20.0
13	KERALA	269	349	29.7	43	34	-20.9
14	MADYA PRADESH	142	282	98.6	55	60	9.1
15	**MAHARASHTRA**	**471**	**681**	**44.6**	**90**	**226**	**151.1**
16	MANIPUR	0	1	@	0	0	@
17	MEGHALAYA	6	17	183.3	0	0	@
18	MIZORAM	0	0	@	0	0	@
19	NAGALAND	0	0	@	0	0	@
20	ODISHA	14	65	364.3	13	39	200.0
21	PUNJAB	72	146	102.8	6	10	66.7
22	RAJSTHAN	147	239	62.6	7	58	728.6
23	SIKKIM	0	0	@	0	0	@
24	TAMINADU	39	54	38.5	2	36	1700.0
25	TRIPURA	14	14	0.0	0	0	@

26	UTTAR PRADESH	205	372	81.5	44	310	604.5
27	UTTARAKHAND	4	23	475.0	0	4	@
28	WEST BENGAL	196	210	7.1	113	132	16.8
	TOTAL (STATES)	2761	4192	51.8	593	1316	121.9
UNION TERRITORIES							
29	A & N ISLANDS	2	18	800.0	0	0	@
30	CHANDIGARH	35	9	-72.7	0	2	@
31	D & N HAVELI	0	0	@	0	0	@
32	DAMAN & DIU	0	1	@	0	0	@
33	DELHI	76	131	72.4	8	19	137.5
34	LAKSHADWEEP	0	0	@	0	0	@
35	PONDICHERY	4	3	25.0	0	0	@
	TOTAL (UT)	115	164	42.6	8	21	162.5
	TOTAL (ALL INDIA)	2876	4356	51.5	601	1337	122.5

Sources: ncrb.gov.in[19]

Pune city Cyber-crime has risen by 39.3 percent within the city recording 319 cases till December 4 2014. Pune police stated that the number of crimes in 2013 was 229 and this year it has increased. They said that social networking websites like Facebook, twitter, mobile apps such as WhatsApp or Hike Messanger have shown highest number [29] of crimes in 2014. Table No. 1.5 shows that Maharashtra has 681 cases registered under Cyber-crime in the year 2013 which is the highest among other states. Table No.1.6 shows Cyber-crime cases in the year 2010-2014 in Pune city. From both the table it is clear that in Maharashtra maximum Cyber-crime occurred in Pune City.

TableNo.1.6: Incidences of Cases Registered Under Cyber Crimes in Pune City during 2010 & 2014

Cyber Crime Year	No of Cyber Crime Registered
2014	319
2013	229
2012	217
2011	307
2010	265

Sources: Pune police Cyber-crime cell [29]

1.5.4 Present Cyber Crime through Public Cyber Cafe:

Cyber Cafe are public internet access point and it is found that public access point are the most liked places by cyber criminals because they can easily hack the Visitors data due to lack of awareness of Cyber-crime in Visitors as well as their identity is difficult to reveal as they are making use public internet point . Many Cyber Cafes are now providing Wi-Fi services for their customers. Due to lack of awareness of cyber security many Cyber Cafe Visitors make mistakes such as making use of unencrypted devices or protocols, not logging out after work is completed, simple password, same password for multiple sites, Information left on the hard drive, not clearing browser history, storing of data on public hard disk, not checking for illegal or malicious software before using public machine which results in loss to the Visitors. In 2013 report by Symantec 56 percent access their social networking account using public Wi-Fi unsecured network, 29 percent access their bank account, 54 percent access personal mail, 29 percent do online shopping, 3 out of 10 do not log off after using public Wi-Fi network and 39 percent do not take any special steps to protect themselves when using public Wi-Fi.

Cyber-crimes can take place when pubic internet access points such as Cyber Cafes are used if security mechanisms are not used. Types of Cyber-crimes that have taken place through Cyber Cafe are credit card fraud by making use of key logger software, online share trading fraud, Email account hacking, phishing, Cyber terrorism, Malicious code like worms, virus etc..

1.6 Cyber Security Scenario in India

Information Technology has grown tremendously in India in last few years and is responsible for growth of individual in every aspect. It helps individuals in every walk of life. Internet users have reached up to 100 million and broadband subscriber has reached up to 12.69 million. India has grown in all leaps and bounds in terms of internet connections to domain name registration and increase in internet service providers. Today India has 134 major Internet service providers,[19] 1 million '.in' domains and 10 million and above registered domain names. Due to increase in internet usage and cyber space activities there is also increase in Cyber-crimes or technological crimes in the country. Along with this lack of discipline from users, inadequate computer and network system protection, lack of Cyber-crime an cyber security management and the anonymous use of ICT – allowing users to hide their identity and also hide their tracks of crime.

Information Technology Act 2000 is a legal framework created and implemented to prevent Cyber-crime and amendments have also taken place for it but still improvements are required. Today Indian cyber space has increase in spam and phishing activities, spread of botnets, virus, worms and malicious code are also on rise. This has made India to be figured out as an active source in spreading malicious infection in computers which is generally observed in developing countries with high rate of ICT usage.

1.7 Legislative Framework for Cyber Crime:

Governments of India have taken various steps for securing cyber space. In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the acceptance of the President in August 2000 was known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.[28]

The Information Technology Amendment Act, 2008 (IT Act 2008) is addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. Indian Computer Emergency Response Team (CERT-In) administer the act. The Act was developed with the intention to prevent Cyber-crime and improve ICT services such as e-governance, commerce different industries were IT is used so that there is growth in economy of the country. It also had security policies in which other countries could collaborate to prevent Cyber-crime. Later the amendment act also came into existence to overcome some security issues not considered in earlier Act along with some new additions of security prevention and legal handling of Cyber-crime. Government has IT Act, National Cyber Security Policy is a policy framework provided by Department of Electronics and Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India.[3]

The initiatives taken by the Government in terms of IT Act as a security framework focused on the issues such as threats to information infrastructure where important data may be stored, threat identification and risk management, switching and using powerful and useful cyber security technology, defining and implementing legal measures to implement and monitor cyber security, making arrangements for training and research to improve cyber security awareness. These government efforts have improved and contributed a lot for securing cyber space and provide a platform for support and growth of cyber security. These cyber security initiatives and actions constantly need to be refined and strengthened frequently.

Features of the actions for protecting cyber space and the level of cyber security preparedness include:

a. Information Technology (Amendment) Act 2008 is created to provide cyber security by taking care of matters such as Cyber-crimes, privacy protection, information infrastructure protection, cyber security and data security.

b. The Indian Computer Emergency Response Team (CERT-In) is a national agency which works as an incident response for team cyber security management. It . It works in collaboration with overseas CERT to improve cyber security management and respond to Cyber-crime incidents so as to prevent it from reoccurring.

c. Public Key Infrastructure (PKI), was established to support implementation of Information Technology Act and promote use of Digital Signatures. Digital signature is a method which has enabled the growth and application of digital signature certificates in a number of areas to protect data from illegal access.

d. In case of emergency for incident response or Crisis for cyber-attacks or cyber terrorisms the National Crisis Management Plan team works out a plan for crisis management. It works along with other critical sectors to prepare and implement a plan.

e. For effective cyber security government follow the Information Security Management System (ISMS) Standard ISO 27001 guidelines for cyber security policy implementation and compliance within government offices and government transaction. In Kolkata a testing facility of IT product for government has been set up which checks the product for certain standards.

f. Security Audit for assessment and risk management are established in various critical sectors of government. These audit will check for threats, vulnerabilities, network design, computer systems, unit and penetration testing, loopholes in system if any etc. This is done periodically so that the critical sectors specially related to economy are not affected by cyber-attack and are prepared to mitigate the attacks.

g. The government has established Research and Development department in the country to form R&D environment. It supports and promote Academic sectors for forming research environment to develop skills to manage cyber security.

h. Many different awareness programs are conducted to spread the awareness of cyber security and information security in the country. For government officials cyber security training facilities are provided to protect cyber-attack and law enforcement agencies are also trained for Cyber-crime investigation

Today most of the information in the world is getting digital form and thus there is also increase in cyber-attacks on this information. Thus there is a need to understand significance and necessity of cyber -attacks and safeguard information by strengthening security to defend against Cyber-crime and cyber-attacks.

1.8 Government Cyber Security Initiatives for Cyber Cafe and its Controlling Authorities

"Cyber security" means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.[28]

Some countries like Japan and Honk Kong there are no law regulating the operations of Cyber Cafes. In Mainland and Taiwan, there are specific legislations regulating the establishment, operation and the use of cyber cafés. In the Mainland, the relevant legislation is the Administrative Measures on Business Establishments that Provide Internet Service, while in Taiwan, it is the Management Provisions for the Information Recreation Industry. In Singapore, operation of cyber cafés is regulated by the Public Entertainments and Meetings Act. In the Mainland, Taiwan [11] and Singapore, network information is scrutinized by the relevant authorities to ensure that the contents are not against the public interest, public morality, public order, public security and national harmony. Contents of computer games are also monitored, since unhealthy contents such as obscenity, gambling and violence are not allowed. Cyber Cafe operators in these three places are required to provide recorded Internet surfing activities for inspection by relevant authorities.

Country like Philippines has ordinance which requires Internet café Owners to, Install filtering software to block adult oriented sites, Prohibit the sales of intoxicating drinks and cigarettes inside their establishment, allow open view of rented computers (i.e. no closed cubicles), Front wall panel is 50% transparent to allow a clear view of the interior of the establishment, adequate lighting both inside and outside of the establishment to allow a clear view of the interior at all times etc.

Internet censorship in Vietnam prevents access to websites [12] critical of the Vietnamese government, expatriate political parties, and international human rights organizations, among others Online police reportedly monitor Internet cafes and cyber law disobeying people have been imprisoned. Vietnam regulates its citizens' Internet access using both legal and technical means. A 2010 law required public

Internet providers, such as Internet cafes, hotels, and businesses providing free Wi-Fi, to install software to track users' activities. Also in 2010, Internet cafes within 200 meters of a school were banned, and those in Hanoi were shut down between 11pm and 6am.

To solve Cyber-crime cases, Indian police developed Cyber-crime investigation cells all over India. These Cyber-crime cell investigates in respect of cases pertaining to hacking, spread of virus, pornography, manipulation of accounts, alteration of data, software piracy, creation of false Web sites, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc..

In order to regulate Cyber Cafes, several states of India government Ministry of communication and Information Technology have passed regulations some under Information Technology Act (ITA) 2000 and some under the State Police Act. Now, the Information Technology Amendment Act, 2008 has made many significant changes in the prevailing laws of cyber space applicable in India, one of which is regarding Cyber Cafes. ITA 2008 has provided a specific definition for the term ‘cyber café’ and also included them under the term ‘Intermediaries’. Several aspects of the Act, therefore become applicable to Cyber Cafes. The government of India has taken initiatives by the mean of Act to provide cyber security for Cyber Cafe. Some of the important points in the Act that are there in the notification of Gazette of India dated 11th April 2011.

- Registration of Cyber Cafe mandatory.
- Identification and authentication of Visitors.
- Maintenance of log for Visitors.
- History of websites accessed using computer resource at Cyber Cafe.
- Logs of proxy server installed at Cyber Cafe, Mail server logs, Logs of network devices such as router, switches, systems etc. installed at Cyber Cafe, Logs of firewall or Intrusion prevention/Detection systems, if installed.[26]
- Minors not allowed unless accompanied by adult

- Physical layout of Cyber Cafe such that all computers face the common open space of Cyber Cafe and partition of Cyber Cafe should not exceed four and half feet from the floor level.
- Illegal content access should be prohibited such as pornography by use of filtering software.

An Cyber Cafe Owner is expected to preserve and retain such information as may be specified for particular duration and in such manner and format as the Central government may prescribe and on failure to do so he may be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine. Thus, the responsibility of Cyber Cafes has now been clearly defined with a three year imprisonment, which is also cognizable, bail able and compoundable.

There are many government stakeholder agencies formed for secure computing environment and adequate trust and confidence in electronic transaction. [Annexure III].

1.9 Present Cyber-crime through Cyber Cafe in India

Computer crime, or Cyber-crime, refers to any crime that involves a computer and a network. There are various crimes that can take place through public computer usage. Some of the Cyber-crimes that took place through Cyber Cafe are listed below.

a) Cyber Stalking

"Infosys techie accuses her colleague of hacking her email account, sending vulgar mails to her friends and posting obscene pictures on social networking sites". [10]

The victim was constantly harassed by attacker through tracking her. Preliminary investigations by the Cyber-crime cell revealed that the mails had been sent from Friends Cyber Cafe in Kothrud.

b) Hacking

"Net cafe staffer held for hacking bank account of customer"[8]

In this Cyber-crime the operator of the Cyber Cafe installed key logger software on all computer system. This software collected all information of the Visitors as soon as they typed from the keyboard. The operator made use of this information for hacking bank details of the victims.

c) **Pornography**

In one of the case the offender obtained group picture of the victim and merged it with pornographic images and transmitted it on internet. The victim was a college going girl and declined to be girlfriend of the offender. The offender made use of more than one Cyber Cafe and it is impossible to find his identity from the emails.[27]

d) **Credit Card Fraud**

In this case a company named Pengengregalo.Com.Ph, based in Makati[1] which delivered gifts to its customer through credit cards was victimized.

In March 2004, the company was victimized by an offender who made use of the e-mail address greedyme@yahoo.com in ordering electronic goods with a large price using fraudulently acquired credit card information. Through investigation it was found that crime was done through Cyber Cafe.

The Internet café was visited but no records were maintained as to its users. The café however has records of time and the corresponding workstation used by customers per day.

e) **Pune Citibank Mphasis Call Center Fraud**

In this Cyber-crime case US customer were victimized by transferring there money from their accounts to bogus account. This was done by the employees of the call center. They made use of Cyber Cafe to conduct this activity. The employee gained confidence of the customer and obtain their pin to commit fraud. They remembered the pin numbers and accessed the accounts. All accounts were opened in Pune. Police has been able to prove that the call center was not at fault and has frozen the accounts where the money was transferred. [6]

There are many other Cyber-crimes such as phishing, Email forging, spoofing , Espionage Email Forging, Intellectual Property Theft, and Denial of service etc. which can take place through public internet access like Cyber Cafe if cyber security is not maintained.

f) State of Tamil Nadu Vs Suhas Katti

The case of Suhas Katti is of major importance because the conviction was achieved successfully within 7 months from filing the FIR. This was the first case of the Chennai Cyber-crime cell. In this the offender Suhas Katti sent defamatory message to the about a divorcee woman in yahoo group. Even emails were forwarded to the victim for gathering information. The posting of messages resulted in annoying messages and phone calls to the lady for solicitation purpose. The victim made a compliant and police traced the offender within few days. The accused was family friend and did this act since the victim refused to get married to him.[9]

Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon’ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe Owners and came to the conclusion that the crime was conclusively proved.

1.10 Chapter Scheme

The chapter scheme for this thesis is as follows:-

Chapter No.	Name of Chapter
1	Introduction
2	Research Methodology
3	Review of Literature
4	Theoretical Concepts of Cyber Security Management System
5	Data Analysis and Interpretation
6	Observations and Findings
7	Conclusions, Suggestions and Scope for Further Research
	Appendices Bibliography

The first chapter is the introduction where the researcher has given a brief background about the study. The second chapter, Research Design and Methodology, has discussed the importance, scope, objectives and hypothesis of the study. It also describes the research methodology and research design. The third chapter deals with the Review of Literature. It describes the review of the existing available literature on the internet, awareness of cyber security. It gives an insight into the history of the internet, cyber security in Cyber Cafe over the years and government rules and regulations for Cyber Cafe. The fourth chapter Theoretical Concepts of cyber security focus cyber security models for successful implementation of cyber security including its awareness and its impact on Visitors. The fifth chapter presents the analysis of the data in two parts, Part –I Cyber Cafe Owner and Part – II Cyber Cafe Visitors. This chapter deals with the testing of hypothesis. The sixth chapter summarizes observations and findings. The seventh chapter provides conclusion and suggestions of the present study along with the framework and scope for further research. References have been given at the end of each chapter themselves and a selected bibliography is given at the end.

References

Sr. No	References
1	Cyber-crime the Upcoming Challenge - Sudan Vision – Independence Daily by Muawad Mustapha Rashid July 11 2007
2	Cyber-crime, Cyber Security And Right To Privacy fifty-Second Fifteenth Lok-Sabha Report http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf
3	Deity published a XII five -year plan on information technology sector Report of Sub-Group on Cyber Security http://deity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf - 2013
4	Gadge Reena K., Dr. Meshram B.B.,"Detect and Prevent Threats in Websites"-IJCST-International Journal of computer science and Techno- vo l. 3, Issue 1, Jan. - March 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)
5	Haseloff Anikar M. - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 - http://ci-journal.net/index.php/ciej/article/view/226/181 - 12/5/2014
6	http://cyberlawclinic.org/casestudy.asp 8/4/2012
7	http://protectmyinternetcafe.com/category/internet-cafes-in-the-developing-world-find-out-what-happens-when-everyone/ 25/11/2013
8	http://timesofindia.indiatimes.com/city/hyderabad/Net-cafe-staffer-held-for-hacking-bank-account-of-customer/articleshow/5357633.cms
9	http://www.legalserviceindia.com/lawforum/index.php?topic=2238.0 7/4/2012
10	http://www.punemirror.in/news/india/Cyber-stalker/articleshow/32718227.cms 2/2/2009
11	Information Note on Regulation of Cyber Cafés in The Mainland, Taiwan, Japan, Singapore and Hong Kong http - www.legco.gov.hk/yr01-02/english/sec/library/0102in34e.pdf
12	Internet censorship in Vietnam article https://en.wikipedia.org/wiki/Internet_censorship_in_Vietnam 3/6/2012
13	Internet Crime Complaint Center (IC3) Published Report on Cyber-crime-2013 http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf 9/11/2013
14	Internet Cyber Cafe - https://en.wikipedia.org/wiki/Internet_caf%C3%A9 - 7/7/2012
15	Internet in India - 2013 - http://www.imrbint.com/downloads/Report-BB55685%20IAMAI%20ICUBE_2013-Urban+Rural-C1.pdf - 8/8/2013
16	Internet users by Year - http://www.internetlivestats.com/internet-users/ - 2012

17 Kumbhar Manisha - Thesis on " Critical Study of Implication of e-governance Services for effective communication with special reference to Citizens in Pune City"-2011

18 Lok-Sabha Published Fifty-Second report standing Committee On information Technology(2013-14) http://www.electroniccourts.in/privacylawsindia/wp-content/uploads/2014/03/Cyber-Crime-Cyber-Security-And-Right-To-Privacy-Fifty-Second-Report-Of-Standing-Committee-On-Information-Technology-2013-14-February-2014.pdf 2/4/2015

19 National Crime Bureau Ministry of Home Affair- Published report on Cyber-crime In India http://ncrb.gov.in/CD-CII2013/Statistics-2013.pdf

20 Pune-Article published on Pune - https://en.wikipedia.org/wiki/Pune-7/8/ 2013

21 Sey Araba, Coward Chris, Bar François, Sciadas George, Rothschild Chris and Lucas Published Research Report on -Connecting People for Development-Why public access ICTs matter-http://library.globalimpactstudy.org/sites/default/files/docs/Connecting%20people%20for%20development%20Global%20Impact%20Study%20final%202013.pdf

22 Sife. Alfred S -" Internet use behavior of cybercafé users in Morogoro Municipality, Tanzania"- Annals of Library and Information Studies Vol. 60, March 2013, pp. 41-50

23 Smart cities Report Published by Symantec 2014- 2015 https://eumartcities.eu/sites/all/files/blog/files/Transformational%20Smart%20Cities%20-%20Symantec%20Executive%20Report.pdf

24 Symantec Published a report on Cyber-crime-2013 - http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf - 11/10/2013

25 The Bombay Police Act - was published in 1951- http://www.humanrightsinitiative.org/publications/police/bombay_police_act_1951.pdf

26 The Center for Internet and Society published an article on CIS Para-wise Comments on Cyber Café Rules, 2011 Internet http://cis-india.org/internet-governance/blog/cyber-cafe-rules 4/6/2012

27 The Committee Appointed By The Bombay High Court published Report on Cyber-crime–January 30 2002

28 The Information Technology (Amendment) Bill, 2008 As Passed By Lok Sabha On 22.12.2008

29 Times of India published an article on Cyber-crime in Pune - 7/12/2014 - http://timesofindia.indiatimes.com/city/pune/Pune-leaves-Mumbai-behind-in-Cyber-crime/articleshow/37591665.cms 30/12/2014

CHAPTER 2

RESEARCH METHODOLOGY

2.1 Introduction

The study is related to the cyber security management for Cyber Cafe in Pune city. The researcher has used survey based research methodology to carry out this research. In this research Purposive, Quota and Convenience sampling method has been used for the purpose of data collection. As per provisional reports of Census [4] India, population of Pune in 2011 is 3,115,431 of which male and female are 1,602,137 and 1,513,294 respectively. For administrative purposes Pune city is divided into four zones which include 14 ward offices. The method of selection of the sample is described in this chapter and after that the nature of primary data and secondary data is explained.

In today's Information Technology world everybody wants to access information at the click of a button. This information may be accessed by using Personal Computer or through Cyber Cafe. During accessing information there are chances of losing data, hacking of data, virus attack etc. Considering the scenario and use of Cyber Cafe, there are chances of loss of data. Cyber Cafes Owners find difficult to manage cyber security and maintain data intact. Considering the importance of information and use of Cyber Cafes there is an urgent need to look out security issues to understand the problems faced by Cyber Cafes and their probable causes for cyber security management.

2.2 Statement of the Study

In today's IT world, technology is moving very fast and due to the competitive environment the mindset of the Internet users is changing equally fast. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. They want secured service at the click of a button to access information and complete their transactions. They can avail this service by using Personal Computer or gadgets or through Cyber Cafe.

The phenomenal growth of Cyber Cafe providing internet services has created the problem of Cyber-crime propagation on the account of investigation difficulties and lack of strong evidences.

Information Technology (Amendment) Act has guidelines for Cyber Cafe. The problem is this statute is more on papers than in execution because Owners and police officers find it difficult to implement it.

Cyber Cafe Owners are aware about cyber security management but find it difficult to implement it. They face many hurdles such as no centralize database for citizens still available, every day new malware growth, maintaining log database for inspection and auditing purposes, internet users expect high cyber security while availing internet service. Other problems like absence of cyber security awareness, lacking to take cyber security precautions, Cyber-crime through Cyber Cafe due to security breaches and gap of communication between government authorities and Cyber Cafe Owners are also there. To bridge this gap it is earnestly necessary to find out a concrete solution for successful implementation of cyber security management in Cyber Cafe.

These problems have drawn attention to research in this area on the topic titled “A critical study of security management system of Cyber Cafes in Pune City.”

2.3 Importance and Significance of the Study

In India Cyber Cafes are used for the purpose of development, entertainment as well as for commerce. Cyber Cafe provides large number of computers accessible to public as compared to other models such as libraries, schools, universities where entry is restricted.

1. Public access mode for information communication and offer a low-cost alternative to the other expensive model at home

2. Cyber Cafes are consequently cheaper access to people who temporarily or generally lack access to internet services.
3. Lowers the multiple financial barriers like investment in the hardware, software, monthly cost, and expenses for updates or security,
4. Provide better equipment or faster connections to enable different and more advanced use.
5. Cyber Cafe functions as center for education and learning new tools which help many people to overcome the skill deficit so that they can access new technologies.
6. In smart cities Cyber Cafe, kiosk, portals, Wi-Fi zone are helpful to carry out information exchange and day to day activities.
7. In recent years Cyber Cafe is used as a gaming center to play online games.
8. In spite of good business opportunity and good money in short time Cyber Cafe business is facing many problems because of the government imposed rule that they need to follow or due to business requirements that they need to do to keep their business running.
9. For Cyber Cafe providing Wi-Fi services, securing wireless communication and Hotspot is required.
10. Identification of various types of risk involved to maintain security in Cyber Cafe.
11. Risk management is essential for vulnerability and threat assessment and their mitigation.
12. Establishment of strong Policies, Procedures and Process to govern Cyber Cafe security.
13. Cyber-crime and Cyber security awareness among stakeholders.
14. Faster crime detection and prevention of Cyber-crime necessary.
15. Lack of trained cyber security manpower.
16. Lack of proper log management for security and inspection process.
17. Use of unauthorized and illegal software damaging hardware and destroying evidence in case of Cyber-crime.

18. Audit and inspection process for cyber security by trained professionals.
19. Performance measurement of auditing and reporting process to better decision making.
20. Advancement in cyber security legislative framework on regular basis.

The Present research work is vital to analyze the security management system in Cyber Cafe. This research will help the Cyber Cafe business process to operate smoothly and security management system will function fast and properly. This research work will draw suggestions which provide benefits to policy makers like governmental agencies and non-governmental agencies for Cyber Cafe.

2.4 Scope of the Study

The study is related to the Cyber Cafe in Pune city. The researcher has considered the Pune urban region for the study. This study is primarily focused on cyber security management awareness and implementation in Pune urban region. Also it focuses on impact of Cyber-crime on Visitor and study and identifies problems faced by Cyber Cafe Owners. The scope of the research is limited to

1. Cyber Cafe –Owners
2. Cyber Cafe - Visitors

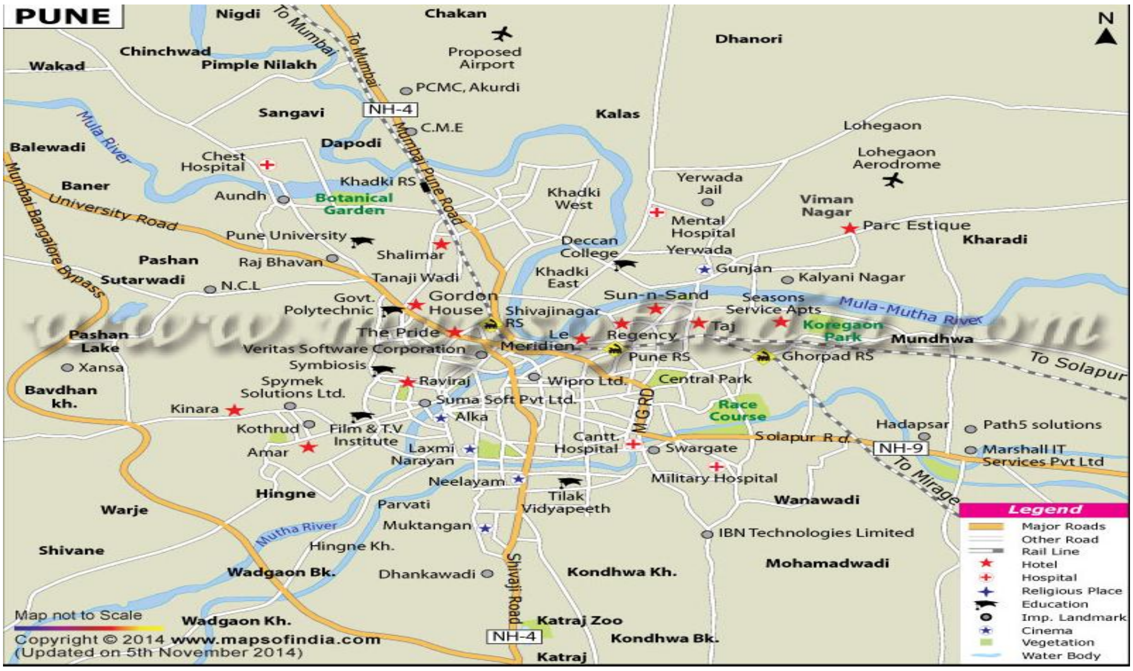
The researcher has considered the Pune urban region for the study since Pune is the second largest city in the western Indian state of Maharashtra. [8] It is known for its educational facilities, having more than a hundred educational institutes and nine universities, as well as its growing industrial facilities. Pune city is an administrative center and now an important industrial hub with reference to IT.

Pune was called "**The Oxford of the East**" by Jawaharlal Nehru, India's first Prime Minister, due to the well-known academic and research institutions in the city. Pune attracts students from every nook and corner of the world. Foreign students find Pune very peaceful and safe compared to other educational cities of India. Pune's economy is driven by its manufacturing industry, although information technology has become increasingly prominent in the last decade. Now Pune is transforming into a vibrant modern city with cafe bubbling activities in the IT and Hi-Tech sectors. Pune is India’s first wireless city. Intel Technology Pvt. Ltd, PMC and Microsense have joined hands to commercially roll out the first phase of a 802.16d Wi-Fi and WiMAX network in the city.

During the course of the present study the researcher has focused on the study of the cyber security in the Pune region as well as on Cyber Cafe Owners to observe how cyber security is implemented and observe awareness of cyber security among Cyber Cafe Visitors.

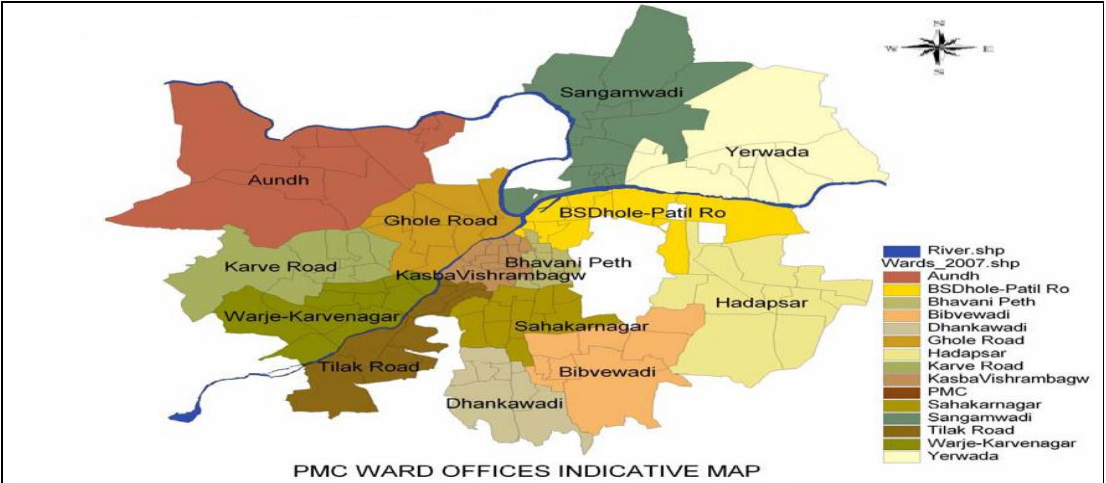
The geographical location of Pune city and ward offices are indicated by the map 2.1 and 2.2 as follows

Map 2.1: Map of Pune city



Source: http://www.mapsofindia.com/maps/maharashtra/pune.htm [6]

Map 2.2 : Map of the 14 Ward Offices of Pune City



Source: http://www.maharashtrafireservices.org/pdf/pune_mitigation_plan.pdf [5]

2.5 Objectives of the study

The Objectives of the research study are as follows:

1. To study the awareness of cyber security management among Owners and Visitors of Cyber Cafe and to study the present cyber security provided in Cyber Cafes by Owners.
2. To observe the impact of cyber security rules and regulations on Cyber Cafe Owners and Visitors.
3. To study the cost benefit analysis for Cyber Cafe.
4. To suggest the effective security system framework to overcome the present problems for Cyber Cafe.

2.6 Hypotheses of the Study

2.6.1 Hypotheses

In consistent with the objectives, following hypotheses were formed by the researcher:

H_1. “Cyber Cafe Visitors are aware about cyber security and fall short to take precautions to avoid Cyber-crime.”

H_2. “The Cyber Cafe rules and regulations have adversely affected Cyber Cafe.”

H_3. “Cyber Cafe Owners feel that there is a lacuna in the audit done”

2.6.2 Description of Hypotheses

1) **H_1. “Cyber Cafe Visitors are aware about cyber security and fall short to take precautions to avoid Cyber-crime”**

This hypothesis has been tested by using the awareness of Cyber Cafe Visitors regarding cyber Security and precautions they take to avoid Cyber-crime. To study the awareness and precaution factors, factor analysis is used to develop concise multiple item scales for measuring various constructs. This test is carried out by using Bartlett’s test of Sphericity which checks the determinant of correlation matrix into consideration which converts it into a chi-square statistics. Another condition needs to be fulfilled before factor analysis would be carried out Kaiser –Meyer-Olkin (KMO) statistics. To study the awareness and precautions to avoid Cyber-crime the cyber security awareness parameters was considered. This parameter is based on the questionnaire of Visitors (Annexure 2 and Question No.9 with 18 factors)

2) **H_2. “The Cyber Cafe rules and regulations have adversely affected Cyber Cafe.”**

This hypothesis has been tested by using the primary data collected from Owner regarding the rules and regulations followed in Cyber Cafe and their effect on Cyber Cafe business. To study the adverse effect of rules and regulations of Cyber Cafe, the parameters such maintaining log registers, type of cubicle and its height, electronically maintained records, document verification, web camera, decline in Cyber Cafe Visitors etc. were considered and Z- Statistics at the 5% level of significance is used. This parameter is based on the questionnaire of Owners (Annexure 1 and Question No.34)

3) **H_3. "Cyber Cafe Owners feel that there is a lacuna in the audit done"**

This hypothesis has been tested by using the primary data collected from Owner regarding the audit done in Cyber Cafe by government official. In this case Z-Statistics at the 5% level of significance is used. This parameter is based on the questionnaire of Owners (Annexure 1 and Question No.40)

2.7 Research Method

This research study is related to the use of Cyber Cafe in Pune city. It utilizes both primary and secondary data. The secondary data utilizes already available information both published as well as unpublished. For primary data however such a facility is not available and it has to be collected by using the survey method. The scope of research is limited. The survey is undertaken by obtaining a purposive and quota sample. The description of the research methodology required for the process of obtaining a sample as well as the nature and size of sample is adequately explained. Purposive, quota and convenience sampling techniques involves the selection of respondents based on the important characteristics under study such as registered Cyber Cafe Owners, Visitors and specific knowledge related to the research problem etc.

2.7.1 Primary data

Primary data are obtained through a survey. Such data is first hand and original in nature. Several methods are used for collecting primary data like telephone survey/e-mail survey, mail questionnaire, personal observation and interviews. Each method has its advantages and disadvantages. The primary data collected by the researcher is explained in the following manner:-

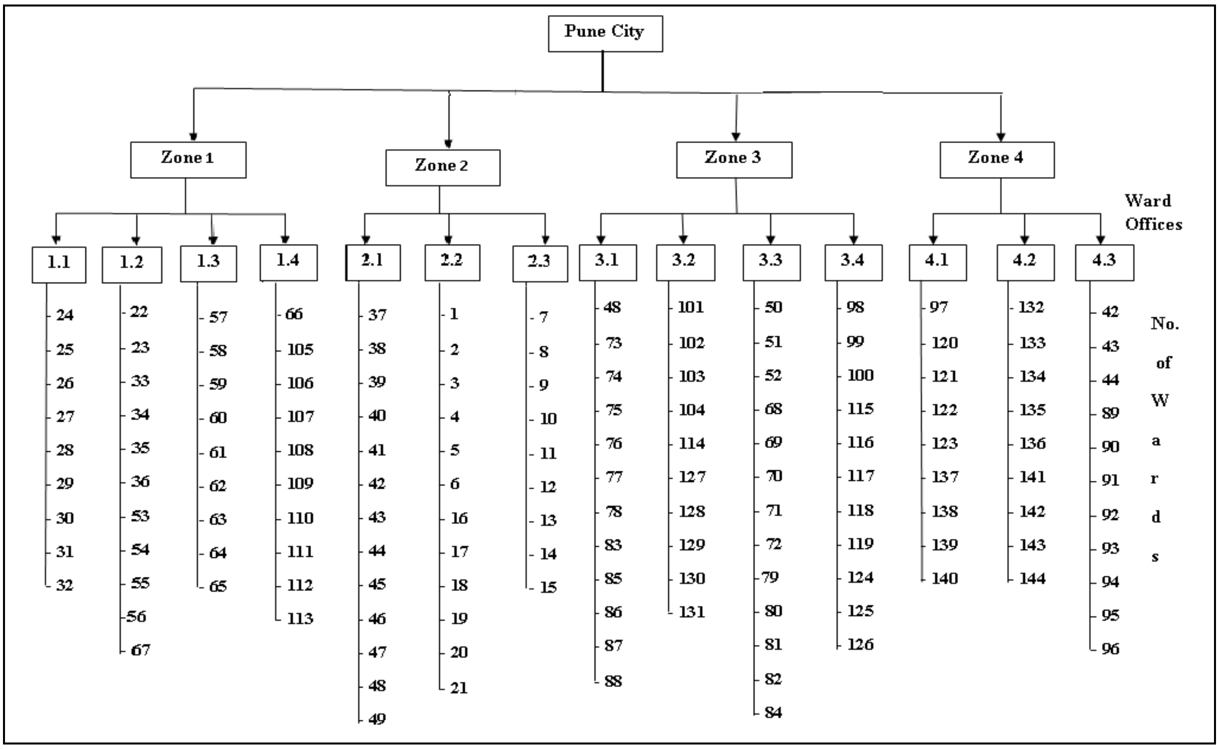
A) Selection of the city

The researcher has used Purposive sampling method to select the city for the purpose of the study. The researcher has selected PUNE CITY as it is “The Oxford of the East" and also a center of IT activity. The researcher has also ascertained that there is scope for the implementation of cyber security in Cyber Cafe in Pune city.

B) Selection of the Wards in Pune City

Pune city is divided into 4 zones and the administrative wing of the PMC is divided into 14 ward offices which include 144 wards. The researcher has used purposive and quota sampling for selection of wards from ward offices in Pune city. In order to study the cyber security in Cyber Cafe, the researcher has located citizens from 14 ward offices [6] from Pune city as shown in Fig 2.1.

Fig 2.1 Ward coverage in the Four Zones of Pune City



Sources: “A Critical Study Of Implication Of E-Governance Services For Effective Communication With Special Reference To Citizens In Pune City- Thesis” [1]

The locations of these specific areas were ascertained for the collection of primary data. (For Ward office Name and Ward Name- Ref. Table No. 2.2)

C) Selection of Sample

This study is related to the cyber security of Cyber Cafe in Pune city which includes the survey related to the Cyber Cafe Owner of Pune city to study the security problems of Cyber Cafe and its impact on Cyber Cafe Visitors and Owner.

The present research is a survey based study of Cyber Cafe of the Owner and Visitors in Pune city. The researcher intends to collect information from Cyber Cafe Owner and Visitors. The purpose of the study is to find out the awareness levels of the Owner and Visitors about cyber security. Also, what are the rules and regulations for the Cyber Cafe? Does it help in cyber security management of Cyber Cafe? To know the details regarding the cyber security management of Cyber Cafe, the researcher has visited many websites and also has visited many Cyber Cafes as a Visitor. In order to attain the above-mentioned objectives, it is necessary to collect both primary and secondary data for the research. The primary data has been collected from

i) Cyber Cafe Owners

ii) Cyber Cafe Visitors.

Table No. 2.1 shows the Sample Design for the study. For the study, sample size for Owners is considered 134 from the Population of size 259. Sampling Method used is Purposive &Quota sampling. For the study, sample size for Visitors is considered to be 384. Sampling Method used is Purposive & Convenience sampling.

Table No. 2.1: Sample Design

Respondents	**Sampling Method**	**Population**	**Sampling Frame**	**Sample Size**
Owners	Purposive & Quota	PMC urban area Cyber Cafe (259) (areas under PMC jurisdiction)	14 Ward Offices	134
Visitors	Purposive & Convenience	Cyber Cafe Visitors	Cyber Cafe Visitors who visit Cyber Cafe	384

D) Selection of the Respondents

In order to study the cyber security in Cyber Cafe, the researcher has located Cyber Cafe Owner from Pune city. Following Table No. 2.2 & Table No. 2.3 shows the total number of Cyber Cafe Owner from 14 wards.

i) Pune Cyber Cafe Owner :

In Pune city, there are 259 registered cyber café in 144 wards. Researcher has considered 134 (more than 50 Percent from each Ward Office) by using **Purposive and Quota sampling method.** Hence researcher has taken the data from respondents from each ward. Researcher has taken the information from the Owners of the Cyber Cafe. The total number of samples selected from respective ward offices from Owner is shown in Table No. 2.2

Table No. 2.2: Ward Wise Sample Distribution of Pune Cyber Cafe Owners

Zone	Ward Office Number	Ward Office Name	Ward wise No. of Cyber Cafe	No. of Owners
1	1.1	Aundh	11	6
	1.2	Ghole Road	12	6
	1.3	Kothrud	9	5
	1.4	Warje and Karvenagar	24	12
2	2.1	Kailashvashi B. S. Dhole Patil	17	8
	2.2	Nagar Road (Wadgaon Sheri)	15	8
	2.3	Sangamwadi	31	16
3	3.1	Bhavani Peth	28	14
	3.2	Sahakarnagar	9	5
	3.3	Kasaba Vishrambagh	17	8
	3.4	Tilak Road	7	6
4	4.1	Hadapsar Ward	19	10
	4.2	Bibwewadi	38	19
	4.3	Dhankawadi	22	11
Total			**259**	**134**

ii) Cyber Cafe Visitors:

In Pune City, there are total 259 registered Cyber Cafes. On an average everyday 60 Visitor's visit the cyber café to avail the services. Hence as per the Krejcie and Morgan Law, if sample size is More than 10 lacs then sample size should be 384. So researcher has selected 384 Visitors from all ward were selected by using purposive and convenience sampling technique. The total number of samples selected from respective ward offices from Visitors is shown in Table No. 2.3

Table No. 2.3: Ward Wise Sample Distribution of Pune Cyber Cafe Visitors

Zone	Ward Office Number	Ward Office Name	Ward wise No. of Cyber Cafe	No. of Visitors
1	1.1	Aundh	11	20
	1.2	Ghole Road	12	25
	1.3	Kothrud	9	30
	1.4	Warje and Karvenagar	24	36
2	2.1	Kailashvashi B. S. Dhole Patil	17	24
	2.2	Nagar Road (Wadgaon Sheri)	15	20
	2.3	Sangamwadi	31	21
3	3.1	Bhavani Peth	28	24
	3.2	Sahakarnagar	9	25
	3.3	Kasaba Vishrambagh	17	19
	3.4	Tilak Road	7	24
4	4.1	Hadapsar Ward	19	40
	4.2	Bibwewadi	38	36
	4.3	Dhankawadi	22	40
Total			**259**	**384**

2.8 Tools for Data Collection

For study purpose, Researcher has collected primary as well as secondary data. Primary data has been collected through Interview and by using questionnaire.

2.8.1 Primary Data: Interview & Questionnaires

i) **Interview**: Interviews were conducted with Ms. Sushsma Chavan, Head Cyber-crime Dept., Pune and Mr. Sanjay Shinde, DCP – Cyber-crime Branch. They have discussed various problems which have been occurred during inspection of Cyber Cafe regarding cyber Security and Cyber-crime such as

- Cyber Cafe Owners do not follows registration norms
- No Centralized Database
- Still Inspection Officers upgrading their knowledge required for inspection for cyber cafe
- Arrange Training Programs for Inspection Officers

ii) **Questionnaires :**

The following steps were used for collecting the primary data.

- Distributing the questionnaire & getting it filled by the concerned respondents. For this purpose an online questionnaire as well as the manual method was used for collecting data.
- Personally visiting the Cyber Cafe for interviews and manual collection of data from Cyber Cafe.
- Personally visiting the Cyber Cafe as Visitors for observation purpose.

Two separate questionnaires were prepared for each of the following groups –

i) Cyber Cafe Owner
ii) Cyber Cafe Visitors

The first questionnaire is meant for Cyber Cafe Owner of Cyber Cafe. It contains information related to their awareness of cyber security and implementation of cyber security methods in Cyber Cafe. It also relates to impact of Cyber Cafe rules [3] and regulations laid down by the government on Cyber Cafe and examines the Owner awareness about cyber security for Cyber Cafe. The researcher has selected Cyber Cafe from only Pune city. It focuses mainly on the cyber security implemented in Cyber Cafe by Cyber Cafe Owner. The researcher will cover only registered Cyber Cafe under Government. The researcher has collected data from various Cyber Cafes in different wards. It also checks how the government does the cyber security checking in Cyber Cafes.

The researcher has applied the following measurement framework for identifying key areas of direct and indirect qualitative impact of cyber security on Cyber Cafe business.

a) Cyber security provided by Cyber Cafe Owner.
b) Cyber security awareness among Cyber Cafe Owner.
c) Security norms followed by Cyber Cafe Owner given by government.
d) Overall assessment of Cyber security management system, related to Cyber Cafe business, satisfaction regarding government rules and regulations in terms of Audit and inspection process etc. are measured on a 5-point Likert scale.

Personal interviews were conducted & questionnaires were filled. The two questionnaires are given in Annexure 1 and 2.

The second questionnaire is for Cyber Cafe Visitors of Pune city. Cyber Cafe Visitors visit Cyber Cafe for many of reasons such as online payments, playing games ,Online buying, Social networking, Shopping , Software usage, e-governance etc. The impact of cybercrime and government rules and regulations on Cyber Cafe is assessed from the Visitors' point of view by studying the problems of cyber security and awareness of cyber security among Visitors. The following framework is used in the questionnaire for the study and it lists the dimensions assessed for Cyber security management.

a) Visitors' awareness about Cyber-crime and cyber security.

b) Awareness about cybercrime and Government rules and regulations for Cyber Cafe Visitors.
c) Problems faced by Cyber Cafe Visitors.
d) Overall assessment of Cyber security management system, related to Hesitation reasons to visit Cyber Cafe, Cyber-crime Awareness, Complaint Registration place etc. are measured on a 5-point Likert scale.

2.8.2 Secondary Data

The Secondary data is used to study the awareness of Cyber security with the help of earlier research studies made by others. It is also used to find out security management in Cyber Cafe. It is helpful to study the objectives and hypotheses framed for the present study.

The secondary data is collected from reputed journals and magazines, newspapers, articles, internet websites and archives. For collecting this data the researcher has visited various libraries. A few of these libraries are Jaykar Library (Pune University), Yashada, Tilak Maharashtra Vidyapeeth Library, British Library, Sinhgad Institute of Management Library.

2.9 Statistical Tools for Data Analysis

The researcher has collected primary data in the field work. Researcher has used various tools like SPSS (Statistical Package for the Social Sciences) package with version 20.0, Ms-Office 2007 (Ms-Word, Ms-Excel), Paint etc.

The Primary data is properly analyzed with the use of SPSS and Ms-Excel. The researcher has used statistical techniques such as frequency distribution, averages, percentages, comparison, and cross-tabulation etc. to analyze the primary data. In addition to this, the techniques of hypotheses testing are also used. Graphs and charts have been also prepared to support the analysis of the primary data wherever necessary.

2.10 Testing of Hypotheses

Testing of hypothesis guides the direction of the research study. It identifies facts that are relevant and those that are not. The hypothesis has been tested on the basis of different statistical tools and criteria. Due to the nature of available data only the criteria norm majority has been used in testing hypothesis. For first hypothesis, Factor analysis is used to develop concise multiple item scales for measuring various constructs. This test is carried out by using Barletts test of Sphericity and Kaiser – Meyer-Olkin (KMO) statistics which checks the determinant of correlation matrix into consideration which converts it into a Chi-Square statistics which indicates that the correlation coefficient matrix is significant as indicated by p value corresponding to the Chi-Square statistics. For second and third Hypothesis, Z-test has been applied with 5% level of significance.

2.11 Time Budgeting

The researcher has concentrated on the duration from 2010-2011 to 2014-2015 to study the Cyber Cafe security management system.

2.12 Limitations of the Study

The researcher being from a technical field may not be able to understand terminologies which are not related to the subject like process of amendment in cyber security law, legal formalities if Cyber Cafe Owners want to run other business along with internet service etc. Since a number of registered and unregistered Cyber Cafes are found in Pune city, expanding the sample frame for the survey had to be restricted in the sample size.

1. The research is limited to only from Cyber Cafe in Pune city due to time limitation in obtaining data across larger geographical area.

2. The research is limited to only the registered Cyber Cafe in Pune city so as to understand whether registered Cyber Cafe Owners are aware about cyber security and how they implement it. Unregistered Cyber Cafes are not considered even though they are in vast numbers.

3. The detail study of role of police in examining the cyber security is not considered for the study but an brief overview is considered for their routine visit to Cyber Cafe as per rules and regulations

4. The other activities such as travel agencies, photocopying, property agents, lottery center etc. was also done by Cyber Cafe Owners who was not focused by researcher since it did not affect the cyber security of Cyber Cafe but were also considered illegal as they were working without license for it.

5. The problem told by most of the Owners related to corruption and bribe by government officers are also not considered since the focus of the study is cyber security.

References

1 Dr. Kumbhar Manisha published her thesis on ‘A Critical Study of Implication Of e-governance Services For Effective Communication With Special Reference To Citizens In Pune City ’- (2012)(http ://Shoghganga.org)

2 http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011

3 http://ddpolice.gov.in/downloads/miscelleneous/cyber-cafe-rules.pdf(5/9/2012)

4 http://www.census2011.co.in (1/1/2013)

5 http://www.maharashtrafireservices.org/pdf/pune_mitigation_plan.pdf (2/5/2012)

6 http://www.mapsofindia.com/maps/maharashtra/pune.htm (23/7/2010)

7 http://www.wipo.int/edocs/lexdocs/laws/en/in/in100en.pdf(12/3/2013)

CHAPTER 3

REVIEW OF LITERATURE

3.1 Introduction

An extensive literature review has been done on the concepts and theories related to the Cyber Security Management. A review of research papers and articles has been undertaken to take note of and acknowledge work that has been done in this field. The researcher has collected secondary data from reputed journals and magazines, newspapers, articles, internet websites and archives. Various libraries in and around Pune City were visited to collect secondary data. The researcher has identified research papers published in renowned journals and conference proceedings along with articles published in newspapers on various topics such as cyber security, Cyber-crime, Cyber Cafe law, impact of cyber security rules and regulations on Visitors and Owners of Cyber Cafe etc. The review of available literature on each topic is taken into account in this chapter.

The researcher has done a literature review on each and every criteria of Cyber security management system. These criteria focus mainly on various aspects of e-governance like-

3.2 Assessment of Cyber Cafe as ICT tool.

3.3 Cyber-crime and Cyber Security aspects and its awareness.

3.4 Government Policy of Cyber Cafe

3.5 Cyber Security Framework for cyber security Management

3.6 Research work on various aspects of cyber security management

3.7 Various articles published in newspapers on Cyber Cafe and cyber security

3.8 Observation of researcher and usefulness of literature review

3.2 Assessment of Cyber Cafe as ICT Tool

1. **Anikar M. Haseloff** have published his article on **"Cyber Cafes and their Potential as Community Development Tools in India"** [17]

In this paper research was conducted to identify the problems and potential of Cyber Cafe as development tools. It finds out the relationship between Cyber Cafe users, their usage pattern and their reach to Cyber Cafe. The author states that Cyber Cafe plays an important role as internet service provider as a shared access point. It effectively bridges the digital divide for the middle class people in developing countries. It helps by helping the users of Cyber Cafe to solve the problems like Social Exclusion by communicating with the people, solving Technological skill deficits, accessing internet services etc. The survey was conducted to study internet usage with respect to time, sectors, Language and place of access. It identifies the age and employment status and education of the Cyber Cafe users. The paper put forth's good point such as Cyber Cafe usage can be measures by not distinguishing between caste, age, sectors and other factors. Even illiterate people can make use of Cyber Cafe without special programs arranged for them to access internet.

2. **Mustafa KOÇ, Karen Ann FERNEDING** has published in their article on **"The consequences of internet café use on Turkish college students' social capital"** [32]

This paper presents the potential impacts of Internet café use on Turkish college students. The author states that internet cafe usage has affected the life of students due to which the students are more interested in online activities rather than spending time with family and friends. Spending of more time at internet cafe has made the students to lead a lonely life and are only virtually connected with the social world. Students prefer to stay online for different purposes. The paper express that internet cafe has changed the youth’s lifestyle. The Cyber Cafe is responsible for youth’s loneliness and lack of social activities. The attachment and belongings of family and friend tie up are reducing due to online relationship which is not face to face and may not be as deep and strong. The internet offers an alternative sphere for social reality which may not exist in reality and may not be authentic. Cyber Cafe works as a complex medium which transfers the social reality into delicate and some time dangerous reality.

3. **Nimmi Ragaswamy** has published in her article on **“Representing the Non-formal: the Business of Internet cafes in India”** [42]

The objective of this research was to explore the small business of information and communication technologies which are deeply embedded in a context of non formal business relations and through an unregulated grey market business practices. This research put forth’s how IT is been used as a formal and non formal form of business. I also reflect how illegal businesses such as piracy are gearing up and are becoming emerging economies. The survey

done reflects that there are many Cyber Cafe which work illegally , not obeying copy right law, not registered, not following the Cyber Cafe law and inappropriate internet browsing is also done. These Cyber Cafe are found as not having proper licensing and Ownership. The Cyber Cafe Owners in Mumbai have found out measures to survive by starting other informal small businesses. The paper focus on Cyber Cafes, especially those sprouting in ‘illegal’ tenements like Dharavi and social practices like youth chatting and gaming lend a new dimension to non-formality. Cyber Cafes have already immersed in non-formal/Para-legal business sociality, becoming sites offering a certain amount of secrecy around virtual dating and flirting for young clients and economic transactions for businessmen.

4. Darlington Onojaefe and Marcus Leaning in their paper on **"Managing Cybercafés: Achieving Mutual Benefit through Partnership"** [27]

In this paper the author place attention placed upon the wider social environment in which the cybercafé operates and the development of 'soft' skills in cybercafé management in order to mitigate security risks. The author focuses on three parts such as Cyber Cafe offers a key for small business may access; second cybercafé will help in relation building in terms of trust and social capital and third to develop such relationships there is a need of new skills sets.

The paper clearly signifies that Cyber Cafe business will flourish if there is partnership with other small business community, government, society and others. It is observed that there are important opportunities for small businesses using ICT which can be successfully grasped, but there are risk that can affect the benefits to be gained. Different types of risk such as illegitimate access, identity theft, and denial of service are constant risk. Through the cooperation and collaboration of all parities in the partnership such risk can be reduced.

5. Bjørn Furuholt and Stein Kristiansen in their paper **"Internet Cafés in Asia and Africa – Venues for Education and Learning?"** [13]

The author in this paper examines the use of Internet cafe in two developing countries; Indonesia and Tanzania. Internet cafe is used for development of wide range of users.

The paper states that for the users, access speed and price are important obstacles to increased use. The author suggests that more research is needed to see how Internet cafés can attract new user-groups to help reduce the digital divide within a developing country.

Internet cafés act as Internet training schools, places for learning, and that they will have a potential to extend this training to a broader area of knowledge with increased capability and contribution from the Internet cafe staff. Training courses, combined with practical use, could be a valuable source for additional income for the Internet café business, and is a useful way to extend the customer base and the market.

6. **Syed Shah Alam , Zaini Abdullah and Nilufar Ahsan** in their paper "**Cyber Café Usage in Malaysia: An Exploratory Study"** [46]

The authors in this paper have studied the pattern of usage of Cyber Cafe in two cities of Malaysia. The paper focuses that in the Cyber Cafe people of all ages and sex come to enjoy the unique, upscale, educational, and innovative environment.

Cyber café seeks to provide its customers with inexpensive Internet access in a comfortable environment. The paper also says that compare to other public Internet access place, Cyber Cafes are playing important role as the most common Internet access place in the urban and rural area in Malaysia. The author observe that a lot of people below 18 years visit the Cyber Cafe and even play online games and Cyber Cafe Owners do not restrict them .

According to research Local government can play an important role in this as well because stricter actions should be taken and punishment should be imposed for not obeying the rules rules. From the study it was observed that younger generations are still not making use of ecommerce in these Cyber Cafes. This reflects that e-business which is important part of globalization, is still not in use in the two cities of Malaysia.

7. **Muhammad MusaudAsdaque, Muhammad Nasir Khan, Dr.SyedAsad Abbas Rizvi** in their paper **"Effect Of Internet On The Academic Performance and Social Life Of University Students In Pakistan"** [6]

In this paper the author has studied the academic performance and social life of university students getting affected by the internet. The paper reflects that use of internet for study purpose and academic achievements are directly proportional to each other while inversely proportional to social life of university students. Different usage of internet by students was studied along with different factors such as social life and outdoor activity. The study explores the correlation of use of internet and social life of university students.

Internet has a strong effect on the students' academic performance but in some cases the social life is inversely affected which needs to be balanced. The Outdoor activities are affected and less time is given for it. Along with Academic performance the social life is equally important which needs to be taken care of.

8. Eshaenana E. Adomi has published paper **"Overnight Internet Browsing among Cyber Cafe Users in Abraka, Nigeria"** [2]

This paper focuses on the overnight internet browsing. The author suggests that cost of the internet access should be reduced so that Cyber Cafe users will make more use of internet. The author finds that the overnight browsing service is a special internet access service rendered by Cyber Cafes in Nigeria to enable internet users access/use of resources and services for longer hours at reduced rates. Also most of the internet users are males and students, the majority of whom use the service to obtain information from the Net for academic purposes which help them to have access to timely, accurate and relevant information.

Seeking academic information from the internet, the net is also used by the students to send and receive e-mail, for entertainment and sports, to read newspapers among other uses. Cyber Cafes are used where they fast computer/internet response can be achieved. Sleep is a problem which most of the users encounter during the overnight internet access service followed by inability to open some sites/web pages.

9. Hemraj Saini, Yerra Shankar Rao, T.C.Panda published their paper on **"Cyber-Crimes and their Impacts: A Review"** [44]

In this paper the authors gives an overview about Cyber-crimes and their impacts over society with future trends of Cyber-crimes. The paper has Cyber-crimes categorized into different parts such as

- Data crime - Data Interception, Data Modification, Data Theft
- Network Crime - Network Interferences ,Access Crime(Unauthorized Access, Virus Dissemination)
- Related Crimes - . Promoting and helping Cyber-crimes to take place, Computer-Related Forgery and Fraud, Content-Related Crime, Cyber sex.

The author has also focuses on the impact of the cyber-crimes such as that there has been an increased rate of prosecutions of cyber-criminals.

There has been an increased fastening down on cyber-piracy related to the film and music works. There are new lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts. Potential Economic Impact, Impact on Market Value and Impact on Consumer trust are also briefed by the authors. The future trends such as if there is a hack into the critical systems in government, companies, financial institutions etc. This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems.

Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently. Cyber Laws, Education and Policy making play vital role and the lack of work required to improve the existing work or to set new paradigms for controlling the cyber-attacks should be considered.

10. Sk. Mamun Mostofa and Shariful Islam has published their paper **"A Snapshot survey of Cyber café users in Dhaka City Bangladesh"** [30]

The paper draw attention to the characteristics of cyber café users in Bangladeshi perspective Cyber café is one of the prevalent ways for people's access to the Internet in poor countries.

The paper shows that that the majority of café users were students. It concludes that people who used the cafés mainly for down loading, reading newspapers and less of them for academic purposes. The respondents mentioned problems of high cost, lower hardware facilities, and slow speed at Cyber Cafes.

Cyber cafés must be regularized under government laws to provide satisfactory standards of service and perk up the environment. Also the environment should also be made favourable for female users and Cyber Cafe must be within reach of all urban and rural residents. Cyber Cafe should be used for learning, education, research, commerce, employment, discussions, exploring the world and other cultures and above all, to make one self-heard. Visitors must have a computer literacy. The government should impose a strict deadline for all ISPs to form set up and to increase Internet bandwidth which can be offered at much cheaper rate. These major benefits could provide and improve access to the Internet for reasonable costs, which could mean lower prices will be paid by cafés for Internet access and eventually users will be charged less for surfing. As a result the Internet could be used more frequently and moreover, more people could access it.

3.3 Cyber-crime and Cyber Security Aspects and its Awareness

11. Jivesh Govil & JivikaGovil published in their paper on **“Ramifications of Cyber Crime and Suggestive Preventive Measures”** [15]

In this paper the author focuses on computer as a crime tool and states that existing laws and preventive measures are not effective to curb such crimes. This lack of legal protection require businesses and governments to adopt solid technical measures to guard themselves from those who would steal, denies access to, demolish valuable information. This paper discusses ramifications of Cyber-crime including discussion on current and emerging forms of computer related illegalities and tools and techniques used in such crimes.

Precautionary measures can be taken by corporate houses and Law Enforcement Agencies including forming of new laws and subsequent issues that arise. Different types of Cyber-crimes and preventive measures have been suggested in this paper so that security systems are up-to-date. Concrete measures must be found in order to track electronics evidence, classify the material that needs to be search, and their preservation, so that systems are better protected from cyber intrusions. In addition, new rules and regulations must be developed by law enforcement agencies to address the various families of computer crime.

12. Derrick J. Neufeld in published [11] in their paper **"Understanding Cyber-crime**"

In this paper the author has analysed 113 U.S. Department of Justice federal Cyber-crime cases from 2008 and 2009, categorizes these cases using an applied criminal offense framework developed by the FBI, considers philosophical explanations for criminal motives, and then identifies the apparent motive(s) that led to the commission of each crime. This paper contributes to an improved understanding of what Cyber-crime is, and why it is occurring at the individual level, in order to develop more proactive and effective solutions. The author provides a classification of crimes such as crime against society, property and crime against person taken from National Incident-Based Reporting System (NIBRS).This paper gives an introduction about the process leading to the crime and specifically the individual's motives to do the crime. Cyber-crimes from various countries such as Canada, US, China are considered. Various philosophical perspectives such as determinism, demonic perspective, for occurrences of Cyber-crime, positivist school, classical school, social perspective etc. are considered.

ICTs are being used to support all type of traditional crimes against people, property and society. ICTs are enabling new forms of crime that are not easily classifiable by existing crime frameworks. ICT-enabled crime can be clearly associated with identifiable, selfish motives. These results indicate that Cyber-crime has a much wider scope than has generally been considered. Furthermore, additional attention must be paid to the prelude stage of Cyber-crime, before the incident occurs or its harmful aftereffects are felt.

13. John Carr has published a paper on **"New Approaches to Dealing with Online Child Pornography"** [8]

In this paper author has shown how the advent of the internet has completely transformed and hugely expanded "the market" for child exploitation images. The paper makes associations between the production and distribution of child pornography and the activities of organized crime. The author concludes by showing that, in relation to the web, there is an efficient system of "notice and take down" which operates very well in many countries but it argues similar systems need to be deployed in many more.

Continued availability of these kinds of images on the internet also contributes to a wider sense that the internet is a lawless place. This in turn inspires more various criminal elements to think of it as an attractive or easy environment in which to operate. It is possible to form a body in every country to specially take care of such crime on internet like Watch foundation in UK. Block list by internet service provider can be made for such websites and stopped for accessing. Also Techniques like Laser Precision can be used.

14. A.B. Patki , S. Lakshminarayanan, S. Sivasubramanian & S.S. Sarma published in their paper on **"Cyber Crime Information System for Cyber-ethics Awareness"** [39]

In this paper the author tells about various crimes such as computer crimes and other crimes. The state of preparedness of governments to face the e-civil disobedience is an area where emphasis on cyber ethics is of primary concern. The government is adopting citizens participation & involvement while making new legislation, mitigating strikes, large-scale scam enquiries etc. Cyber-crime Data Base Services will be useful in providing deeper insight into the functional dependencies of crime rate, ethical issues, and social and cultural practices of society. The micro level and macro level database need to be created for offences/crimes for providing query services. Such database access to Cyber-crime information need to be given to law enforcement agencies, the social reformers and psychologist along with law enforcement agencies. A partial view of the information system which can be implemented with the support of UN is discussed in this paper.

Different types of Cyber-crimes include hacking, password trafficking, violation of copyrights, online pornography, Denial of Services (DOS) attacks and any other crimes committed using a computer network or computer system such as crimes affecting online transactions relating to ecommerce, credit card thefts, cyber stalking, cyber defamation, cyber terrorism etc. must be studied and taken actions against them. Micro level and macro level Cyber-crime database services should be created. Database Services have to attract public to utilize the services of portal by increasing awareness about cyber security and availability effective services.

15. Alex Roney Mathew, Aayad Al Hajj & Khalil Al Ruqeishi has published in their paper **"Cyber Crimes: Threats and Protection"** [29]

The authors discusses various types of Cyber-crimes and the ways to protect them with special emphasis on biometric. Cyber-crimes such as phishing where various methods such as DNS Cache poisoning, link manipulation, filter evasion, graphical substitution, email spoofing, and pharming are discussed. Problems and protection methods such as not clicking on online unknown links, not opening unknown sender email, using protective methods such as biometric finger print, palm geometry, signature, retina, iris and facial expressions etc.

Various countries should make cyber law stronger and international organization should come forward to stop cyber-crime and protect consumers.

16. Sanjay Bahl, O P Wali and Ponnurangam Kumaraguru has published paper on "**Information Security Practices Followed in the Indian Software Services Industry: An Exploratory Study"** [7]

In this paper the authors examine the security gaps in software services outsourcing from a vendor perspective. Indian software service vendors provide service delivery to their customers with respect to security as an integral part of their services, which is critical from a trust, relationship building and business sustainability.

To improve the overall information security practices in a supply chain, the acceptable service quality as defined and perceived by the customer needs is to be raised to a higher level both within their own organization and at the service provider end. The service providers in the supply chain should explore the process of self-attestation wherein they lay out the practices and the required activities to claim so they have a balanced business model for information security thereby helping create more secure outcomes.

17. Gregory White & Natalie Granado has published a paper **on Developing a Community Cyber Security Incident Response Capability** [47]

The paper focuses on the cyber-attack and its response paper. The author feels that the response process should be in the event of a cyber-attack on a community is not addressed. Community leaders do not have direct control or authority over the many disparate organizations within a community but may reasonably be expected to direct the response to such an attack. This paper addresses this issue and makes various recommendations for what community scan do in preparing for a community response to a cyber-attack or incident. This paper suggested several steps that communities could take that would start the community on the way to establishing an incident response capability and a security program which would enable them to potentially prevent or detect, respond to, and recover from a cyber-security attack.

The need for communities to have a viable cyber security program is growing. Also as more and more government functions become available to citizens online, the potential for the disruption of these services also increases. E-Government can't exist without e-security. There is a lot of guidance on developing an incident response capability for organizations. Community Cyber Security Maturity Model which can serve as a roadmap for both states and communities in their efforts to build a cyber-security program and capability.

18. D. Nitzberg has published in his paper on **"The Cyber Battlefield - Is This the Setting for the Ultimate World War?"** [35]

According to the author the motivations for war are different in the cyber environment where the focus is one of information piracy and information system vandalism. To look after the international cyber-crime there is no proper legislation made. The author also states that because the internet network society is new and evolving, many do not understand information security issues and are find it difficult to protect information and information systems which provide an opportunity for cyber criminals to cause disaster. The author suggests that organizations must form their own information intelligence groups. These will study the computing systems, both planned and in-place, identify the salient security issues, and take formal steps to resolve them. Then, measures will be taken and updated to maintain the security infrastructure of the organization. To build on this, corporations with like-minded infrastructures can exchange information within coalitions or bodies to disseminate information towards assisting in preserving the integrity of their secure infrastructures. Thus by actively implementing measures to address both internal and external security threats, the majority of information warfare incidents can be mitigated.

19. Andrea Rigoni, Igor NaiFovino, Salvatore Di Blasi has published in the paper on **Worldwide Security and Resiliency of Cyber Infrastructures: The Role of the Domain Name System** [43]

The aim of the author is to focus on critical infrastructure like power plants, energy grids, oil pipelines and DNS infrastructure. The cyber-criminal can make use of the vulnerabilities to exploit DNS and affect cyber infrastructure operation. Framework for the development of a DNS health Assessment framework which is internationally coordinated initiative and promoted by GCSEC is presented. DNS factors such as availability, integrity, security, speed and stability are considered along with vulnerabilities and threats are considered for the framework.

Threats are classified into two main categories data corruption, denial of service and privacy. Impact of threats on DNS Health and security is also discussed.. To improve the security a international community level DNS at different levels such as technical level, operational level and policy level is considered. Framework provided by GCSEC-Global Cyber Security Center is discussed which is intended to support risk analysis and impact analysis of changes to the DNS infrastructure.

20. **Goran N. Ericsson** has published in his paper on **Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure** [12]

In objective of this paper is power system communication (PSC) and cyber security. PSC and cyber security issues are vital parts of the critical information infrastructure, such as a smart grid system. Here a historic perspective has been given, tying up PSC and cyber security. Also, the development fully integrated computer environments has been described. The digital threats are increasing which need to be handled. Physical security is considered and is quite mature. Classification of communication in three categories is done such as real-time operational communication requirements, administrative operational communication requirements and administrative communication requirements. Cyber security issues such as De-Coupling between Operational SCADA/EMS and Admin IT, to Secure Operational, Threat and Possibilities, SCADA Systems and SCADA Security Governmental Coordination in Sweden on SCADA Security, Information Security Domains are discussed.

21. Kweku K. Arthur, Martin S. Olivier, Hein S. Venter & Jan H.P. Eloff has published in their paper on **"Considerations Towards a Cyber Crime Profiling System"** [5]

In this paper a framework for an integrity-aware Forensic Evidence Management System (FEMS) is developed. In an effort to automate the analysis process, this system would provide investigators with a holistic view of the forensic evidence at hand, thereby providing insights into the quality of investigative ,inferences. A finite state automaton (FSA) is used to model the behaviour of the FEMS. The FEMS considers assisting investigators in addressing investigative challenges. The components of the FEMS were described, and a finite state automaton (FSA) was utilized to model and reason around the FEMS behaviour. Sample rules within the rule state of the FSA were put to identify specific Cyber-crimes.

22. Lawan Ahmed Mohammed has published his paper **"Cybercafé Systems Security"** [26]

The paper introduces the vulnerability and security issues associated with the use and operations of internet cafes or Cyber Cafes. The paper puts forth the challenges faced by those operating and managing Internet cafes, government ,parents and even educators to ensure proper preventive measures, guidelines and laws needed to protect the system against breaches misuse and abuses. It also discusses that defense mechanism against breaches should be dynamic and strong enough due to the increasing number of new freely available cracking tools and harmful Web sites. The author discusses different defense mechanisms for virus, worms, Trojan horse, adware, malware, and spyware.

Only using antivirus, firewalls and intrusion detection techniques are not sufficient enough to protect the entire system. For securing Cyber Cafes management system must conducting regular testing for systems vulnerabilities, employing a process to proactively monitor systems activity and take proper action when any attempt is made to illegally gain access to the system, cooperation with authorities and law enforcement agencies. Etc. It is essential to note the cafe administrator needs to plan and consider the specific requirements in the context of their own network, environmental, appropriate policies, and economical factors. For future scope it is suggested that study on how to enhance coordination and awareness between the general public and different entities involved in legal and ethical issues regarding the use of Internet is required.

23. **Adetoun A. Oyelude** and **Cecilia O. BolajokoAdewumi** "Cybercafe Physical and Electronic Security Issues" [38]

The author in this paper provides an overview of physical and electronic security issues in cybercafes in Ibadan city, Nigeria. The author has also explained about various types of crimes Unauthorized access, Hacking, Cyber terrorism, Cyber talking and online harassment Fraud and identity theft, including phishing, Information warfare ,Denial of service attack, Malicious code and virtual crime, such as the theft of virtual property. Security measures should be followed to protect the systems and ensuring that all government rules and regulations are followed. The author emphasis on providing security at all levels such as physical security in which access restriction and verification should be considered so that unauthorized data access is prevented, appropriate action should be taken if an intrusion occurs without permission. Operational level security must be implemented by providing authentication mechanism like password and user id. The cafe Owners should monitor Visitors visiting at night they should maintain tables to aid privacy of clients as well as maintain cyber security. The Visitors must get themselves well trained so they are able to make use of internet service properly. Security measures should be followed by the Visitors of the Cyber Cafe to prevent and avoid cyber attack. Law enforcement agents should be trained for cyber security.

24. Alex Ozoemelem Obuh has published paper on “**Viruses and Virus Protection in Cybercafes**” [36]

The objective of this paper is to give an insight to virus, virus infection, and prevention in cybercafés. Specifically, it gives the meaning of virus, types of viruses, classification of viruses, sources of viruses in cybercafés, and reasons as to why cybercafé systems are vulnerable to attacks or infections. It also discusses sources such as computer programs, Java and other Internet /Word–Wide-Web script, embedded code, source code, secondary devices, etc. responsible for virus infection. The author focuses on So Big-F virus and suggests that the governments of the countries where most viruses are created should be pressed to pass the appropriate legislative measures.Detection of virus infections or symptoms of virus infection in cybercafe systems or networks, virus prevention and control must be done. It is argued that with the advent of Wi-Fi technologies, virus writers can insert malicious code from just about anywhere in the world, and as such there exist a form of cyber-terrorism that cannot be easily stopped.

25. Odumesi John Olayemi has published in his paper “**A socio-technological analysis of Cyber-crime and cyber security in Nigeria”** [37]

In this paper the author focused on impact of sociological and technological factors on Cyber-crime and cyber security and expresses the relevant circumstances and threats of Cyber-crime from theoretical and investigative points of views. The author has briefed about four crime theories Structural Functionalism Theory, Marxian Theory, Routine Activity Theory and Technology Enabled Crime Theory which were all found to be relevant to Nigerian Cyber-crime. The author express that currently there are no existing laws to handle Cyber-crime directly. The author has studied various theories and briefed about it such as structural Functionalism Theory, Routine Activity Theory, Marxian Theory, The Theory of Technology-Enabled Crime etc.

Existing criminal laws should be reviewed for cyber security threats, establishment of Forensic laboratories, capacity building programs for law enforcement agencies, development of cyber security technology framework etc. Cyber-crime policy should be evidence based along with efforts should be considered at international level to get funding so that practical implementation is possible. Cyber-crime awareness should be improved among public.

26. Longe, O.B., Chiemeke, S.C. and Longe, F.A. has published paper on **"Intermediary Mediated Cyber-Crime: Internet Access Points And The Facilitation Of Cyber-crimes In Nigeria"** [28]

In this paper the author has investigated Internet access point through which Cyber-crimes can occur and found the level of involvement and IAP role in Cyber-crime activities done in Nigeria. The author states that Internet pornography has increased to a larger extent through Cyber Cafe along with spam mail forwarding, malicious software, lottery scam and many other are done through Cyber Cafe. The author suggest that there is necessity to be proper cyber security measures that need to be followed abiding with the law. The Cyber Cafe Owners and users must be aware about cyber security and strict actions must be taken for those who do not follow the norms.

27. Abdul Rahman Garuba has published his paper **"Computer Virus Phenomena in Cyber Cafe**" [1]

The paper examines the concepts, history, sources, spread, detection, and removal of computer viruses. The paper focuses on Computer viruses and computer security vulnerabilities. The author suggests that Cybercafé managers should have a good understanding of the risk and controls associated with various security technologies. It is the hope of the author that adequate awareness and understanding of the destructive devices by

Cyber café managers and computer users generally will help secure their systems. It is recommended that cybercafé administrators develop a security policy for both employees and users.

In case of wireless connectivity the Visitors should ensure that if laptops or handhelds are used they must be configured by your own 128-bit WEP encryption and additional layers. Laptops must be required to use BIOS password for start-up. Finally, cybercafé administrators and operators should visit regularly the computer emergency response team (CERT) which is regarded as perhaps the Internet-best known security organization. For data integrity, Security awareness, training, and education and focus on the audit of internal and external networks should be done.

3.4 Government Policy of Cyber Security

28. Kaustubh Phanse and Hemant Chaskar,.Pravin Bhagwat has published their paper "**Complying with DoT Regulation on Secure Use of Wi-Fi: Less in Letter, More in Spirit**" [41]

The author in this article throws light on Wi-Fi security. The paper focuses on Department of Telecommunications (DoT), Government of India, recently published Regulation (dated February 23, 2009) outlining the procedure for secure use of Wi-Fi. DoT's efforts in ensuring secure use of Wi-Fi are creditable and at least two positive outcomes can be seen. One it will trigger a nationwide awareness drive about Wi-Fi security. Two it will compel ISPs, enterprises, and end users to take Wi-Fi security seriously.

Unless Wi-Fi users implement the suggested Wi-Fi security best practices locally, centralized authentication alone will not serve the purpose DoT is trying to achieve. The author also focuses on bodies such as the Indian Computer Emergency Response Team (CERT-In) and the Data Security Council of India (DSCI) can play an important role in creating awareness about these best practices. ISPs should tell their subscribers to implement good cyber security practices and should also ask them for compliance process. Doing so will allow ISPs to truly secure Wi-Fi Internet access across their subscriber base, while relaxing the stringent requirement of centralized authentication.

29. Danielle Kriz has published his paper "**Cyber security Principles for Industry and Government"** [25]

In this paper the author has given six principles to improve cyber security. The author suggest that in order to have continued viability of the infrastructure and growth of their sector, technology companies are highly motivated to design and build security of their products and systems. For economic growth and protection the governments need to secure global information infrastructure. It is required to enhance cyber security at a global level and efforts should be taken on that line. Risk management should be considered to avoid security breaches and crimes.

30. Prashant Iyengar has published article on **"IP Addresses and Expeditious Disclosure of Identity in India"** [24]

In this research, Prashant Iyengar reviews the statutory mechanism regulating the retention and disclosure of IP addresses by Internet companies in India. The author provides a compilation of anecdotes on how law enforcement authorities in India have used IP address information to trace individuals responsible for particular crimes. The author has given various examples in this article as to how IP address was used to trace the cybercriminal. Along with successful cases some mistakes done by the police have also been listed in his article.

For proper tracking of crime case it is required to implement Unique Identity Numbering Scheme and the Centralized Monitoring System.

31. Samuel Samuel Chiedu and Avemaria Utulu has published their paper **"Enhancing Social Security through Appropriate Cybercafé Security Policy in Nigeria"** [9]

In objective of this study is to development of appropriate Cyber Cafe security policy in Nigeria. It explains how cybercafé security policy can be used to reduce criminal activities perpetrated in Nigerian cybercafés against individuals and organizations who use the Internet for various business transactions. The author suggests that cyber security policy should be a part of National Information Policy and should cover both technical security needs and social security needs to benefit from highly from the highly electronized modern business environment. According to the author the proposed cybercafé security policy should have factors such as: Technology requirements that are type of hardware and software requirements, Entrepreneurship, Cyber Cafe commission and Users sensitization etc.

Technical and social policy like technical Firewalls Intrusion detection Anti-virus protection Auditing and Integrity testing Encryption and for social Identify critical information sector Vulnerability and risk assessment Policy formulation Education and training Strategic Intelligence management should be considered. Proper implementation of Cyber Cafe security policy in Nigeria will be of help to both local and international communities. The policy, once well implemented, will enable organizations and individuals use the Internet without discrimination. It will also make other international communities that have not trusted Nigeria in the past to develop trust and thereby start dealing with Nigerians online.

32. **Stella E. Igun** published paper on **"Cyber Crime Control in Developing Countries' Cyber Cafes"** [23]

This paper discusses the challenges and problems governments and other stakeholders are facing infighting and controlling Cyber-crimes in developing countries cybercafés. The main focus of this paper is on the developing countries vulnerability to Cyber-crimes. Author feels that these countries lack major infrastructural devices for controlling Cyber-crimes at the moment. The author notes that the Cyber-crime rate is high and global (affecting the developing countries all the same) and the developing countries are still very low in Internet connection. The paper reveals reasons for the increase in the incidences of Cyber-crimes in developing countries, Cyber-crime laws that have been enacted to control and tackle the problem of Cyber-crimes are also highlighted. In this paper author has elaborated steps for cyber security laws taken by various countries and focuses that in current situation the industrialized countries have their own laws of cyber security and crime like the U.S. is leading in the area of Cyber-crime laws, the European Union countries are next to the industrialized countries in the subject of Cyber-crime law's enactment. Developing countries are just getting started in the subject of Cyber-crime laws and this is very pathetic. The author suggests that there is a gap that exists between the developed countries and the developing countries in the subject of Cyber-crime control and security which must be bridged immediately.

The developing countries should unite with the governments of the developed countries to bridge the gap by following the guidelines that have been laid down by theG8 countries and the European Union. The final goal should be to make sure every country in the world should participate in the Cyber-crime control and in the electronic community.

33. **Sara M. Smyth** has published article on **"The Greening of Canadian Cyber Laws: What Environmental Law can Teach and Cyber Law can learn" [**45]

In this article the author examines whether Canadian environmental law and policy could serve as a model for Cyber-crime regulation. The focus of this Article is on the problem of data security breaches, which target businesses and consumers. The article provides an overview of the parallels that can be drawn between threats in the natural environment and on the Internet and the current situation of Cyber-crime threats in Canada, as well as the Canadian government's regulatory response. The author suggest a model for effective cyber security which has different steps such as Identify and characterize/classify the following, Risk Identification, Determine Likelihood and Impact of Risk, Develop a Risk Management Policy and Set Targets/Goals, Develop On going Compliance , Monitoring and Audit Procedures, Establish Response Procedures for Issues Affecting Customers and information Sharing and Reporting

Policy-makers can lead a great deal from these efforts about the kinds of laws and policies that might be workable in the cyber-realm. The paper also examines what specifically cyber-law theorists and policy-makers can learn from those in the environmental law field.

34. Government of India regulation under ITA- Information Technology Act – 2000 and Information Technology Amendment Act, 2008 [14]

In order to regulate Cyber Cafes, several states of India government Ministry of communication and Information Technology have passed regulations some under Information Technology Act (ITA) 2000 and some under the State Police Act. Now, the Information Technology Amendment Act, 2008 has made many significant changes in the prevailing laws of cyber space applicable in India, one of which is regarding Cyber Cafes.

ITA 2008 has provided a specific definition for the term ‘cyber café’ and also included them under the term ‘Intermediaries’. Several aspects of the Act, therefore become applicable to Cyber Cafes. The government of India has taken initiatives by the mean of Act to provide cyber security for Cyber Cafe. Some of the important points in the Act that are there in the notification of Gazette of India dated 11th April 2011 such as Registration of Cyber Cafe mandatory, Identification and authentication of Visitors, Maintenance of log for Visitors, History of websites accessed using computer resource at Cyber Cafe, Logs of proxy server installed at Cyber Cafe, Mail server logs, Logs of network devices such as router, switches, systems etc. installed at Cyber Cafe, Logs of firewall or Intrusion prevention/Detection systems, if installed, Minors not allowed unless accompanied by adult, Physical layout of Cyber Cafe such that all computers face the common open space of Cyber Cafe and partition of Cyber Cafe should not exceed four and half feet from the floor level, Illegal content access should be prohibited such as pornography by use of filtering software.

An Cyber Cafe Owners is expected to preserve and retain such information as may be specified for particular duration and in such manner and format as the Central government may prescribe and on failure to do so he may be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine. Thus, the responsibility of Cyber Cafes has now been clearly defined with a three year imprisonment, which is also cognizable, bail able and compoundable.

3.5 Cyber Security Frameworks for Cyber Security Management

35. National Institute of Standards and Technology has published article on **"Framework for Improving Critical Infrastructure Cyber security** [33]

In this article framework for cyber security by US government is given. The framework was created in collaboration with private sector which use common language to address and manage cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses

The framework guides cyber security activities for business. It consists of three parts: he Framework Core, the Framework Profile, and the Framework Implementation Tiers.

The Framework helps organizations in terms of degree of cyber security risk, regardless of size – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides the organization to structure today's cyber security problems by following standards, guidelines, and practices that are working effectively in industry today. The model can serve as a model for international cooperation on strengthening critical infrastructure cyber security.

36. Kevin P. Newmeyer has published his paper on "**The FATF as a Model for Internet Governance**" [34]

In this paper the author has elaborated organization and operation of the FATF in its role as an international organization opposing a security threat and shows how a similar organization might be effective in improving global cyber security governance. The Financial Action Task Force (FATF) was created in 1989 to counter money laundering with a structure that is flexible and adaptable to address emerging challenges such as terrorist financing and proliferation financing.

The countries following this model are required to Investigate and prosecute money laundering and financial crimes, Deny criminals access to their illegal gains, Place a burden on financial system service providers to implement controls for due diligence, suspicious activity reporting, and record keeping, Implement oversight mechanisms to ensure susceptible businesses and professions comply, Improve transparency for legal persons to ensure accurate Ownership information is available to authorities, Establish international cooperation and information sharing mechanisms.

37. Department Of Information Technology published article on "**National Cyber Security Policy**" [10]

The Department of Information Technology has proposed a draft for National Cyber Security Policy for secure computing environment and adequate trust & confidence in electronic transactions which has focused on Security of cyber space, enabling the Process, Enabling technologies – Deployment and R&D, Enabling people and Responsible actions by user community. These factors consider information gathering from multiple sources and monitoring of real time assets that need protection and adequate expertise and process to deal with crisis management. For this trained and qualified manpower along with suitable incentives are required. A conceptual model to be designed for this purpose is discussed in this draft. The draft also discuses about Information security Assurance Framework', including creation of national conformity assessment infrastructure. This framework will guide in creation of National conformity assessment infrastructure.

3.6 Research Work on Various Aspects of Cyber Security Management

38. Hamid Salim has published his thesis on "**Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks**" [16]

The Researcher in his thesis has focuses on traditional methods for managing cyber security risk and proposed new method for managing cyber security risk more effectively. The researcher finds that traditional methods used have become ineffective and in his thesis he has proposed a new method for managing cyber security risks based on a model for accident or incident analysis, used in Systems Safety field. The model proposed by the researcher is called System - Theoretic Accident Model and Processes (STAMP). It is rooted in Systems Thinking and Systems Theory. Based on a case study specifically written for this thesis, the largest cyber - attack reported in 2007 on a major US based retailer, is analysed using the STAMP model.

In this paper TJX cyber-attack is also discussed. It also provides suitable measure to be taken to avoid cyber attack. Further, STAMP generated specific recommendations for managing cyber security risks more effectively.

39. Petra Raisanen has published his thesis "**THE URBAN TECHNOSPACE A Study on Internet Cafés in Shanghai**" [40]

In this thesis the researcher indicate that the main motivation behind the Internet café use was entertainment and that the Internet use in the cafes was ritualistic, habitual and pleasure-seeking. For the urban youth culture, the Internet cafes provided a space where the youngsters could reinforce their identities as trendy, technology-savvy urbanites. The researcher finds that the youth of Shanghai are exposed to globalization and foreign values via all aspects of their consumerism. Alongside of the food, clothing and entertainment, the Internet is one of the major channels of diffusing foreign values in to the country.

New media culture gives the urban youth the means to values as freedom and individualism. The users supported the government's points of view in restricting access of the minors to the cafes, or setting limits to the time spent inside. Support for restricting access to “harmful” sites and was strong.

40. Akinola Azeez Paul and Chong Zhang has published thesis on **“Evaluate Security on the Internet Cafe”** [3]

In this thesis the researcher has taken case study to provide solution to the problems encountered by the network users such as Internet Game Centre (Centrum Halmstad, Sweden) and, the Blueville Internet Cafe (Ede, Nigeria).The cybercafé threats require a constant security monitor of computer infrastructure. The monitoring system against threats is very important in today’s global communication. The monitoring system should deliver real time service and improves the performance of the infrastructure (equipment) by actively analyzing the logs and message alert. The researchers strongly suggest use of WPA2 using 802.1x which is difficult to crack. The author also suggests that users are inclined to damage and errors that resulted in a large risk in today's computing.

Proper education and awareness should put in place that can govern how we use and manage wireless networks.

41. ZurianiBt Ahmad Zukariai published his thesis **“A Framework For Ethical Usage Of ICT Services At Cyber Cafe Using Theory Of Planned Behavior”** [48]

In this research the researcher as proposed a framework for an ethical usage of ICT services at the Cyber Cafe. The researcher has used quantitative and case study research approaches, where the first part involved a survey method to determine the variables that influence the user's behavioural intention on unethical usage of ICT services at Cyber Cafe. The respondents for these were Cyber Cafe operators, Cyber Cafe users, regulatory bodies, parents and community. The second part used a case study approach to further examine the effectiveness of the control mechanism through the implementation of monitoring software. This study used Theory of Planned Behaviour as the theoretical framework of the study. In order to examine the behavioural intention of Cyber Cafe users, an additional variable known as external factor has been added in the conceptual framework of this study. The researcher found that attitude, subjective norms, perceived behavioural control and external factors have a significant relationship with behavioural intention of Cyber Cafe users. Experience, individual rights, peers, teachers, close friends, CC TV, lighting in the Cyber Cafe and noise in the Cyber Cafe are proven to have influenced behavioural intention of Cyber Cafe users to perform their actions. Based on the findings, the researcher has developed a framework for an ethical usage of ICT services. The researcher suggests that this framework could be used by Cyber Cafe operators, authorities, and policy makers in planning and implementing any strategies and policies for Cyber Cafe operation in Malaysia.

42. **Ms.Magacha** has published thesis on **"Role of Cyber security Strategy on Citizens Security: Approaches to Improve Public Awareness on Mobile Internet Threatsin Kenya"** [31]

In this research work the researcher has studied the role of cyber security strategy on citizens security and has explored approaches to improve public awareness of mobile threats. The Participants for the study were taken from the KICTANet listserv who were surveyed over a four week period through an online survey tool. The study confirmed the occurrence of mobile Internet threats with participants suggesting awareness drives to empower the public to improve on detection and easily accessible security – related technology and law enforcement were also proposed as ways to reinforce the awareness drives targeting different sectors of society. It is also suggested that the government should focus on national awareness drives to target all users on mobile Internet. For achieving this the media and public campaigns can be used , carrying out national surveys on cyber security awareness to identify the gaps that would inform the awareness drives, supporting the public with information on threats through institutions can be done.

43. Alaeldin Mansour Safauq Maghaireh has published his thesis **“Jordanian Cyber-crime investigations: a comparative analysis of search for and seizure of digital evidence”**[4]

In this research work the researcher examines cases associated with the Cyber-crime investigation done by Jordanian law enforcement officers performing searches and seizures of computers. The study focuses on the inefficiency and ineffectiveness of traditional Jordanian laws for considering the Cyber-crime investigations. Details related to crime investigation are studied by the researcher and also compared the procedures and methods with Australia and the USA. The researcher has tried to put guidelines for strengthening of search and seizure procedures in Jordanian Cyber-crime investigation. The researcher has given guidelines such as for issuing a cyber-search warrant what should be considered like probable cause, subject of the search warrant, scope of the search warrant, also how the execution of cyber search warrants should be done, who should accompany the officers executing the search etc. The researcher also throws light on Cross border searches and seizures.

3.7 Various Articles Published in Newspapers on Cyber Cafe and Cyber Security

44. “ Noida police launches new software to check cyber crimes” [21]

To ensure cyber security in the city, Noida police directed 70 Cyber Cafe Owners to install new software that will secure their computers from being misused. Noida police in association with Ideates Innovations launched a new software 'iCafe Manager' to be installed in computers to check Cyber-crimes.

Deputy Superintendent of Police (Crime) Triveni Singh said that Cyber Cafes in Noida can avail this software free of cost and improve the user experience along with assisting in national security by securing their cafes. According to Triveni Singh the objective is to ensure cyber security and management in Noida city. The software helps in user data storage, accounting, terminal management and providing a convenient environment for users. The software can capture Digital photo, name, address and photo ID archive data can be easily searched without any problem of storage Singh added. DSP said that the 'iCafe Manager' software is accordance with the new Information Technology Act Rules, 2011 under the IT ACT.

45. **"Cyber Cafe Owner being questioned for alleged terror links"** [20]

A Cyber Cafe Owner was detained by the police as emails were sent from his cafe and were alleged terror links. The terror groups were found convicted in Krishna district. The Owner had not maintained proper details of the Visitors so were questioned. Krishna district Superintendent of Police D Ramakrishnaiah said about this.

46. **"Growth of Cyber Cafes declining sharply"** [19]

In this article the factors responsible for decline in Cyber Cafe are put forth. As per CII-IMRB Broadband report the Cyber Cafe growth rate has fallen by almost 20% in 2008.The reason for this mainly told by cafe Owners were harassment by local police and unwanted government paper work that they have to do and follow. The article also stated that in some cities like Pune, it is requires to take permission from a municipal health department to open a Cyber Cafe, just because cyber has got a 'cafe' suffixed to it. Since the literal meaning of a cafe is a place to have coffee and snacks. Also in the country, the local police has to provide a no objection certificate in order to open a Cyber Cafe. As per Internet Service Providers Association of India (ISPAI) Rajesh Charria the other reason for decline is maintaining a log of all sites visited by a customer along with their identification proof. He added that the local police interference should be removed and proper security management should be implemented. He also felt that the government's laws are discriminatory towards Cyber Cafe.

47. “Cyber Cafes ordered to install CCTV cameras” [18]

According to this article it was found that a threatening email to Dera Sacha Chief Gurmit Ram Rahim Singh sent from a local Cyber Cafe the it was ordered to all Cyber Cafe Owners in Sirsa district that they have to install close circuit TV cameras in their premises. The police added that they noticed that Owners were not maintaining proper records of their Visitors like their complete address, contact number, names, percentage, and duration for which the internet was used so this order was passed.

48. “Testing time for Cyber Cafes” [22]

According to this article Cyber Cafes are getting closed and main reason for it is the internet penetration at household level at low cost. The cafe Owners are taking precautions to prevent Cyber-crime. Cyber Cafe which are still in business are making money by holding online study centres and examinations, arranging video conferencing between companies and even matrimonial alliance management for families.

3.8 Gap Analysis and Observation of Researcher with Usefulness of Literature Review

The researcher has been benefited from these Reports, Articles, Research papers and it was observed that there exist gap between existing study work done and the proposed study. The literature review explored the effectiveness and evaluation of cyber security for Cyber Cafe and concluded that most of the studies done are at micro level and not at macro level for Cyber Cafe as a whole. The researcher found that there is a strong need for broad and specific approaches of cyber security management of Cyber Cafe which would help in implementation of better cyber security for not only in Cyber Cafe but at all public internet access points and places. Through the Literature review the researcher found that studies related to cyber security management for Cyber Cafe were not conducted nationwide or internationally. Not a single study focuses on all aspects of Cyber Security management system for Cyber Cafe and a framework for it. They only focus on various aspects of such as

- Cyber-crime, Cyber Security and Cyber Threat & Protection
- Cyber Cafe as development tool, venue for education and Learning
- Business of Cyber Cafe formal and Non formal
- Cyber-crime frameworks for cyber security in general for all organizations
- Rules and regulations for Cyber Cafe and Cyber security policies.
- Managing Cyber Cafe and its Usage, Impact of internet on society
- Cyber ethics, Cyber Security measures, and precautions
- Role of different Domain Name System and Broad Band Wi-Fi Regulation
- IT Act and Amendment Vulnerability and Threat management

The Researcher has done extensive Literature Review and was able to identify various **gaps and issues** in the area of cyber security management for Cyber Cafe which are listed below:

- Visitors information which is vital part is not given highest priority.
- Personal and sensitive information of Visitors is vulnerable to Cyber-attacks.
- Till today there does not exist centralized database for citizens in Cyber Cafe so that by making use of system like biometric identity could be proved.
- Government officials focus on Log collected and stored by Cyber-cafe Owners as per the Rules and Regulations which may not be sufficient.
- The infrastructure and security is not considered seriously.
- There is strong need of security framework for Cyber Cafe security management.
- There is no way listed in law to improve the awareness of cyber security among Owners of Cyber Cafe to prevent Cyber-crime.
- The lack of regular updating of law for cyber security is a big problematic issue.
- Proper auditing process methods are still not reflected in law to identify risk and vulnerability.
- Reliable, timely and specific information on cyber security management for Cyber Cafe is still not available.
- A common and proper channel is still missing between Cyber Cafe Owners and

Government officials to discuss issues related to Cyber Cafe security management

In this research study the researcher has considered different cyber security aspects for Cyber Cafe. It focuses on the impact of rules and regulations for cyber security on Cyber Cafe Visitors and its Owners. The different types of crime and how to handle them are considered. The government role for cyber security is studied along with other stake holders from private sectors are also considered. Awareness about security and Cyber-crime plays an important role which is considered for Visitors and Owners. By considering suitable cyber security measures there will be less Cyber-crime and it will be helpful to the government officials to track the crimes. The visitor's awareness plays an important role in the cyber security of Cyber Cafe. In addition to above literature, many other articles have been reviewed. Researcher has defined different aspects which are shown in the following Table No.3.1, which is further used for designing questionnaires.

Table No. 3.1: 20 Aspects of Cyber Security Management System.

Cyber Crime Reduced	Risk Mitigation	Threat Identification	Cyber security Awareness	Improvement in Cyber Security Law Amendment
Effective Cyber Security Implementation	High Clarity and simplicity of processes	Security Of Data	Improvement In reputation of Cyber Cafe	No hesitation to visit Cyber Cafe
Improvement in Cyber Cafe Business	Faith of Visitors in Government cyber security Handling	Symbiotic Relationship between Owners and Government Official(Police)		Improvement in Cyber Cafe Usage
Improvement in Auditing process	ICT Globalization	Satisfaction of Visitors and Shopkeepers	Improvement in identification of crime	Less Corruption

References:

Sr. No	References
1	Adomi Eshaenana E., “The Journal of Community Informatics”, http://ci-journal.net/index.php/ciej/article/view/322/319,2007
2	Akinola Azeez Paul and Chong Zhanghas, thesis “Evaluate Security on the Internet Cafe” , http://www.divaportal.org/smash/get/diva2:608536/FULLTEXT01.pdf
3	Alaeldin Mansour Safauq Maghaireh, Thesis “Jordanian Cyber-crime investigations: a comparative analysis of search for and seizure of digital evidence”, http://ro.uow.edu.au/cgi/viewcontent.cgi?article=4404&context=theses - 2009
4	Arthur Kweku K., Olivier Martin S., Hein S. Venter & Jan H.P. Eloff, The Third International Conference on “Availability, Reliability and Security”,ISBN- 0-7695-3102-4/08 IEEE, DOI 10.1109/ARES.2008.107
5	Asdaque Muhammad Musaud, Khan Muhammad Nasir , Dr.Syed Asad, Rizvi Abbas, “ Journal of Education and Sociology”, ISSN: 2078-032X, December, 2010
6	Bahl Sanjay , Wali O P and Kumaraguru Ponnurangam, , “ Coalition on Internet Safety”, Second Worldwide Cybersecurity Summit,WCS 2011, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber- 978-0-615-51608-0/11 ©2011 EWI
7	Carr John , “Children’s Charities’, “ Coalition on Internet Safety”, Second Worldwide Cybersecurity Summit, WCS 2011, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 EWI
8	Chiedu Samuel and Avemaria Utulu, “InformatIon scIence reference-Security”, ISBN 978-1-59904-905-2 (e-book)
9	Department Of Information Technology, http://deity.gov.in/content/national-cyber security-policy-2013
10	Derrick J. NeufeldRichard, Proceedings of the 43rd Hawaii International Conference on “System Sciences -2010”
11	Ericsson Goran N. IEEE- “ Transactions On Power Delivery”, VOL. 25, NO3, July 2010
12	Furuholt Bjorn, Kristiansen Stein, “The Journal of Community Informatics”, www.ci-journal.net/index.php/ciej/article/download/314/352 - 2007, ISSN: 1712-4441

13 Garuba Abdul Rahman , "Information Science Reference", ISBN 978-1-59904-905-2 (e-book)

14 Government of India regulation under ITA- Information Technology Act – 2000 and Information Technology Amendment Act-http://deity.gov.in/content/information-technology-act- 2008

15 Govil Jivesh, Govil Jivika , "Electro/Information Technology", 2007 IEEE International Conference Proceeding, E-ISBN :978-1-4244-0941-9 Print ISBN: 978-1-4244-0941-9, -2007

16 Hamid Salim, Cyber Safety: Thesis "A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks " http://web.mit.edu/smadnick/www/wp/2014-07.pdf

17 Haseloff Anikar M. "The Journal of Community Informatics ",IEEE,UNIVERSITY Vol-1 No.3 2005

18 http://articles.economictimes.indiatimes.com/2008-07-02/news/27734377_1_cyber-cafes-cctv-cameras-sirsa, PTI Jul 2, 2008, 04.32pm IST

19 http://articles.economictimes.indiatimes.com/2008-07-15/news/27697952_1_cyber-cafes-sify-naresh-ajwani, Harsimran Singh, ET Bureau Jul 15, 2008, 08.05am IST

20 http://articles.economictimes.indiatimes.com/2008-12-03/news/27704863_1_terror-links-cafe-krishna-district, PTI Dec 3, 2008, 02.29pm IST

21 http://articles.economictimes.indiatimes.com/2012-12-30/news/36063564_1_cyber-cafes-check-cyber-crimes-cyber-security, PTI Dec 30, 2012, 10.57PM IST

22 http://www.thehindu.com/news/cities/chennai/testing-time-for-cyber-cafes/article1718950.ece, June 6, 2013 14:22 IST

23 Igun Stella E. http://www.igi-global.com/chapter/cyber-crime-control developing-Coutries/28543 ISBN 978-1-59904-905-2 (e-book)

24 Iyengar Prashant , http://cis-india.org/internet-governance/front-page/ip-addresses-and-identity-disclosures

25 Kriz Danielle- Global Cyber Security Policy, Information Technology Industry ,Second Worldwide Cybersecurity Summit WCS 2011 -http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 -EWI

26 Lawan Ahmed Mohammed, "Security and software for cyber cafes", InformatIon science reference, ISBN 978-1-59904-905-2 (e-book)

27 Leaning Marcus ,Darlington Onojaefe "InformatIon scIence reference"-https://books.google.co.in/books?isbn=1599049058

28 Longe, O.B., Chiemeke, S.C. and Longe F.A, https://www.intgovforum.org/cms/documents/contributions/general-contribution/2008-1/349-longe-o-b-et-al-isp-and-Cyber-crime-in-nigeria-igf-contributions/file

29 Mathew Alex Roney, Hajj Aayad Al, Ruqeishi Khalil Al, International Conference on “Networking and Information Technology”, 2010

30 Mostofa Sk. Mamun and Islam Shariful, “Research Journal of Recent Sciences” ISSN 2277 -2502 Vol. 2(3), 53-58, March(2013), http://www.isca.in/rjrs/archive/v2i3/9.ISCA RJRS-2012-421.pdf - Res. J. Recent Sci

31 Ms.Magacha, Thesis “A Framework For Ethical Usage Of ICT Services At Cyber Cafe Using Theory Of Planned Behavior” http://www.kictanet.or.ke/wp- content/uploads/2014/11/Role-of Cybersecurity-on-Citizens-Security-FINAL.pdf

32 Mustafa Koç, Ferneding Karen Ann, “The Turkish Online Journal of EducationalTechnology - TOJET”, July 2007 ISSN: 1303-6521 volume 6 Issue 3 Article 9

33 National Institute of Standards and Technology - http://www.nist.gov/cyberframework/upload/cybersecurity-021214-final.pdf. February 12, 2014

34 Newmeyer Kevin P. , Second Worldwide Cyber Security Summit, WCS 2011 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 EWI

35 Nitzberg S. D. , “ International Symposium on Technology and Society, U.K”, Proceedings of the 1997, ISBN:0-7803-5538-5,Volume-1 , http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=822776&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D822776

36 Obuh Alex Ozoemelem, “Security and Software for Cybercafes”, DOI: 10.4018/978-1-59904-903-8.ch011, http://www.irma-international.org/chapter/vi1ruses-virus-protection-cybercaf%C3%A9s/28536/

37 Odumesi John Olayemi, “International Journal of Sociology and Anthropology IJSA ” , Vol. 6(3),pp.116-125, March, 2014 DOI: 10.5897/IJSA2013.0510 ,ISSN 2006- 988x , http://www.academicjournals.org

38 Oyelude. Adetoun A. , Cecilia O. Bolajoko Adewumi, “Security and Software for Cybercafes” http://www.igi-global.com/chapter/cybercaf%C3%A9-physical-electronic-security-issues/28531, DOI: 10.4018/978-1-59904-903-8.ch006 (ebook)

39 Patki S A.B., S Lakshminarayanan, S.S. Sivasubramanian , Sarma,Proceedings of the 2003 “ International Conference on Cyberworlds”, (CW’03)0-7695-1922-9/03 $ 17.00 © 2003 IEEE

40 Petra Raisanenhas, Thesis “The Urban Technospace A Study On Internet Cafés In Shanghai”, http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1327545 &fileOI d=1327546) 2006

41 Phanse Kaustubh and Chaskar Hemant,. Bhagwat Pravin http://www.airtightnetworks.com/fileadmin/pdf/Implementing_DoT_Regulation_on_Wi-Fi_Security.pdf

42 Ragaswamy Nimmi ,“International Conference on Ethnographic Praxis in Industry” EPIC 2007 Proceedings - EPICZW7,pp 115 127, ISBN 0 97990942 2 02007

43 Rigoni Andrea, NaiFovino Igor , Blasi Salvatore Di , Second Worldwide “Cyber Security” Summit WCS 2011, ISBN: 978-1-4577-1449-8, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 5978795-8-0-615-51608-0/11 ©2011 EWI

44 Sain Hemraj i, Yerra Shankar Rao, Pand.T.C, “ International Journal of Engineering Research and Applications (IJERA)”, ISSN: 2248-9622 Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209, www.ijera.com

45 Smyth Sara M. , “International Journal of Cyber Criminology” Vol 8 Issue 2 July December 2014

46 Syed Shah Alam , Zaini Abdullah and Ahsan Nilufar , “Journal of Internet Banking and Commerce”, April 2009, vol. 14, no.1 - http://www.arraydev.com/commerce/jibc/)

47 White Gregory, Granado Natalie ,Proceedings of the 42nd Hawaii International Conference on “System Sciences”– 2009 ,978-0-7695-3450-3/09 $25.00 © 2009 IEEE

48 Zuriani Bt Ahmad Zukariai, Thesis “A Framework For Ethical Usage Of ICT Services At Cyber Cafe Using Theory Of Planned Behavior”, (http://etd.uum.edu.my/2815/2/1.Zuriani_Ahmad_Zukarnain.pdf)2011

CHAPTER 4
THEORETICAL CONCEPTS OF
CYBER SECURITY MANAGEMENT SYSTEM

4.1 Introduction

Cyber Security management system is the immune system in the management of Cyber Cafe. Cyber Cafes play an important role in businesses that engage in e-business. They are the main access point for internet users. According to CCAOI Cyber Cafes are growing in the country with its users [13]. The various trends, the growth and the different players in the market mark its prominence. With the availability of tools that helps translate English language content into the local languages, the Cyber Cafes, in fact, are empowering the population in remote locations across the country. Incidentally in a recent survey it was observed that India to become second –largest internet market in 2014 out of which the Community Service Centers and Cyber Cafes are the main point of access for 40 percent of them. With the advent of growing nature of information communication through Cyber Cafe there is a need for cyber security management for Cyber Cafe. [2] The Cyber Cafe owners extend the freedom of use of Internet access to the community but they find it difficult to tighten their Cyber Cafe cyber security to safeguard the private information of their customers. Cyber security threats destroy the value of Cyber Cafe. In a democratic country like India the government respect online or internet freedom for this the need for cyber security is becoming more and more prominent. Cyber Cafe requires elucidations at various levels of cyber security such as Physical level security, Operational level security, Application level security, Database level security and Network Level security through technical standards. It requires solutions by both government and non-governmental organizations. The cyber security policy processes for Cyber Cafe must be based on the principles of openness, collaboration, and a respect for human rights in a democratic country to protect social security of the citizens.

Lots of efforts are being taken on the cyber security front for Cyber Cafe by the government. Due to the growth in Cyber-crime attacks and fear of getting victimized by cyber criminals and stringent government Cyber Cafe laws the visitors hesitate to go to Cyber Cafe. To improve the Cyber Cafe business at a greater extent there is a need to reconsider the cyber security management implemented currently in Cyber Cafe so as to remove the hesitation of visitors. Better cyber security management and security policy for Cyber Cafe, better Cyber Cafe business will be there.

4.2 Cyber Cafe Cyber Security Management Terminologies

To manage the Cyber Cafe cyber security various terms need to be understood with their role and significance.

4.2.1 Cyber Cafe

Cyber Cafe means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

Caslon Analytics show three models for Cyber Cafe

1. Some Cyber Cafe will provide only basic connectivity for necessary work such as checking email. Such venues are generally used by tourist or by people who need to do some urgent transactions. These venues may have 10 to 20 pieces. Such places will generally not provide food items and beverages. The customers over here are random customers and not regular.
2. The second model is a venue which provides different services along with CD burning, printing, scanning, binding, photocopying and many more. The visitors over such places are regular visitors who come for many activities such as bank transactions, chatting, research and many others. Also such venues provide food and meals ranging from snacks to full meals. Such venues are generally used by youngsters and people for some office work.

3. The third model is used as a gaming zone where multiplayer games among users are played. These require connectivity from different venues. Such models require different game playing equipment's such as joystick, headphones or speakers. It requires higher configuration machines and high speed internet connectivity.

   Now days wireless hotspots i.e. allowing visitors to access the net without using someone else machines is also a popular model. Cyber Cafe owners find it attractive model because they are free from hardware and software maintenance. In the west many companies have realized that Cyber Cafe can be best place to sell their products since customers get a chance to use computer software or hardware before making the purchasing decision and thus making an educated decision. These products are either available at the Cyber Cafe or via on-line storefront.

4.2.2 Computer Network Primer

Computer Networks are used to share resources, requesting and providing services and exchange or transfer information/data. The classifications of computer networks are generally done on the basis of geographical area that they cover as shown in the Figure No. 4.1.

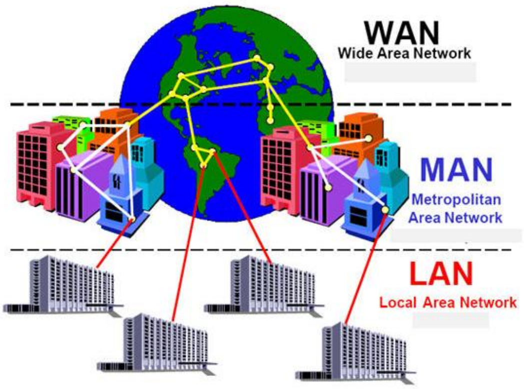
LAN: a Local Area Network typically covers a smaller geographical area. It can transfer data at a very high speed among host. It connects hosts which are only a few kilometers away from each other. Example offices, school building.

MAN: a Metropolitan Area Network typically interconnects host at larger distance as compared to LAN. E.g. connecting different cities.

WAN: a Wide Area Network covers larger geographical area. It can be anywhere on the earth. Public telephone network, Satellites or leased lines are used for WAN. Example: Internet.

Traditional hub-based Ethernet (wired) LAN's as well as IEEE 802.11 wireless LAN's (commonly called Wi-Fi) use broadcast communications. This means that packet (or frame) between two nodes can be read by all other nodes on the LAN. Thus eavesdropping on private communications in such LAN's is relatively straight forward and hard to detect.

Fig 4.1 : LAN, MAN & WAN



Sources: http://www.solucionwifi.com.ar/images/ /LanManWan.jpg

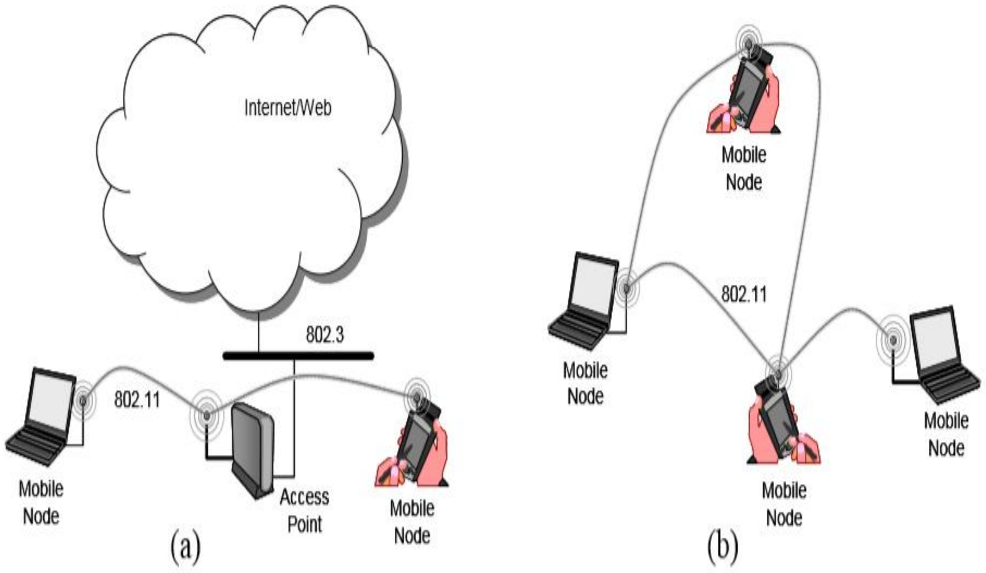
A Wireless local-area network (LAN) connects different hosts such as laptops, machines, devices to the internet. Wi-Fi hotspots at Cyber Cafe allow internet connection for visitors by connecting to Cyber Cafe business wireless network.

A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications.

Depending on whether or not there is a fixed infrastructure, wireless systems can be categorized as either ad hoc networks or infrastructure systems as shown in Figure No 4.2 . Infrastructure systems have fixed network resources in the form of a base station or access point (AP), which performs central administration for multiple mobile stations. The base station routes packets between mobile nodes, which do not communicate directly with each other. Infrastructure systems are organized in cells, which reuse portions of the spectrum to increase spectrum usage at the expense of greater system infrastructure. Base stations may have high-bandwidth connections to wired infrastructure networks. There is no direct ("peer-to-peer") communication between users. Rather, each mobile station sends its message directly to the base station in its cell, and this local base station routes.

Ad hoc networks [9] have no pre-existing (fixed) infrastructure and the network architecture is configurable. They are formed by wireless stations which may be mobile and they route paths for each other. Every station in an ad hoc network can be set up as, and play the role of, a base station where it can directly transmit and receive from other stations in the network. Packets may need to traverse multiple links to reach a destination. Due to the mobility, the routes between stations may change dynamically. Ad hoc network can co-exist and co-operate, i.e., exchange data packets, with an infrastructure-based network.

Fig: 4.2 IEEE 802.11 Wireless LAN-(Wi-Fi)



(a) Infrastructure “cellular,” and (b) infrastructure-less ad hoc systems, both based on IEEE 802.11 wireless LAN, also called Wi-Fi.

Sources: Wireless Network Local and Ad hoc Network- Ivan Marsic

4.2.3 Cyber Security

Officially, ISO/IEC 27032 [14] addresses “Cyber security” or “Cyberspace security”, defined as the “preservation of confidentiality, integrity and availability of information in the Cyberspace”.

Authentication, authorization, and non-repudiation are tools that are used to maintain system security with respect to confidentiality, integrity, and availability. Understanding each of these six concepts and how they relate to one another helps to design and implement secure systems. Each component is critical [7] to overall security, with the failure of any one component resulting in potential system compromise.

The term confidentiality means Protection of information from unauthorized access to unauthorized individuals systems or entities. The term integrity means protection of information, system and services from unauthorized modification or destruction and the term Availability means availability or reliable access of data and information services in a timely manner.

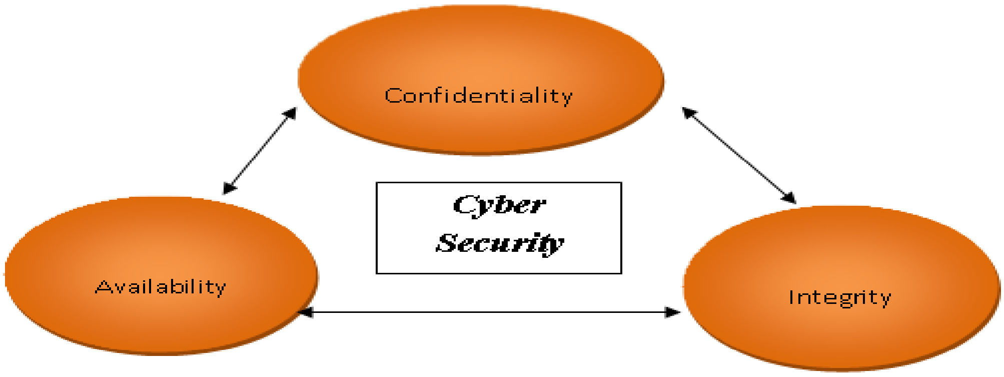


Fig 4.3: The Components of Cyber Security

In turn “the Cyberspace” (complete with definite article) is defined as “the complex environment resulting from the interaction of people[6], software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

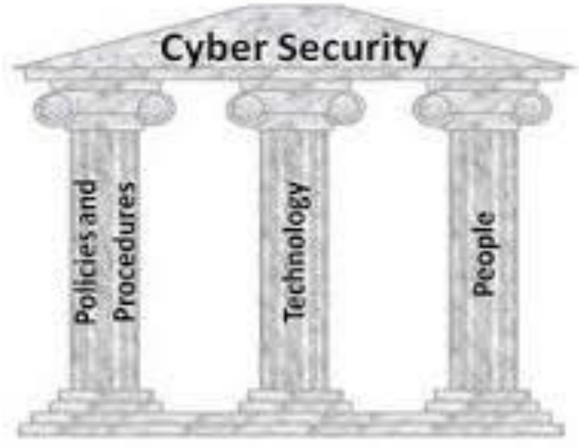


Fig 4.4: The Three Pillars of Cyber Security

A stable [1] physical structure requires at least three main supports. Industrial cyber-security is no different. It requires supporting structures for a stable system. Three “pillars” form the basis for an effective cyber security system: technology, policy and procedures, and people.

The first pillar is technology which deals with identification of users, authentication of users and system and access control for users and system. Various techniques used for this are implementation of firewall ,data encryption, intrusion detection systems, network access control systems , wireless network security [15], virus protection software, time controlled resource availability, gateways etc.

The second pillar of a cyber-security system is a set of well-defined and readily available policies and procedures. Policies and procedures define how to use technology for implementing security in an effective manner. Technology security solutions operate, evaluate and configure cyber security system. It identify the risk, vulnerabilities management cost and risk associated to it.

The Third Pillar is the trained and motivated workforce. This is the important pillar because even if great technology or best policies are there and if people are not comfortable with it or not able to use it then there is no use of it. So people should be trained and there should be awareness among the society of cyber security.

Cyber security refers to the technologies and the process designed to protect computer networks and data from unauthorized access, vulnerabilities and attacks delivered via the internet by cyber criminals [5]. It is a process of applying security measures to ensure confidentiality, integrity and availability of data. It encompasses Preventing detecting and responding to cyber-attacks.

Cyber Security is a hierarchy of security layers as shown in Figure No. 4.5. The base layer is the physical security which protects from physical access to the assets. The next layer is operational security which protects assets to be hampered from unauthorized access. The next layer is the software security layer which consists of system software security or application software level security. Protecting software layer will protect from virus, malware, botnets or other breaches which are illegal. The next layer is the database layer security which protects from loss of confidentiality and availability of the data. The top layer is the network layer which protects the network components, connection and content on the network from illicit means of accessing it. There are different means and methods to implement cyber security at each layer.

Physical Security Layer:

Physical security is implemented by protecting the physical assets. Physical security refers to the protection of building sites and equipment [16] (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls under physical security layer.

Operational Security Layer:

Operational Level security is implemented to protect the cyber-attack breaches at operational level. In many cyber control domains there are inherent trust and privileges that exists. At such places access control needs to be applied at operational level for all the users. For a robust access control points that should be considered are: managing user access and user responsibility, monitoring operating system control and directing device access control, assigning privileges to users and designing a proper robust access control function. The person who is going to monitor the operations should have sufficient knowledge to handle security problems.

Software Security Layer: The two main categories of software are system software and application software. System software is a program which governs working of computer itself such as the operating system and utilities. Application software is software which perform specific task of the users such as MS-office, Visual Studio, etc. Software security is implemented at two levels at System software level and Application software level. At system software level Within the operating systems of some of the specific control system components (Human-Machine Interface computer [HMI], Front-End Processor [FEP]) [17], certain controls must be in place to ensure instructions are being executed in the correct security context. Most operating systems have mechanisms that restrict the execution of certain types of instructions allowing him to occur only when the operating systems of the control system components are in a privileged or supervisory state. This protects the overall security and state of the control system and helps to ensure it runs in a stable and predictable manner. Application security level [3] security is to protect application software from external threats. Software security is becoming increasingly important concern as applications become more frequently accessible over networks and are as a result vulnerable to a wide variety of threats. Different security measures for application level security are application firewall that limits the execution of files, routers which prevent the IP address to be directly visible on the internet of a computer, encryption /decryption programs, spyware detection/removal programs and some authentication software systems such as biometric. Providing the application level software security is necessary to keep threats such as Denial-of-service (DoS) attack, malware such as virus, adware, spyware etc. Applying a patch for system software and application [3] software at regular interval will keep the vulnerabilities such as malware away from the system.

Database Security Layer: Database security concerns the use of a broad range of information security controls to protect databases [12](potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. The threats to database are loss of integrity, confidentiality and availability. The different security risk at this level is malware infections causing leakage of information, deletion or damage to data, denial of authorized access to the database, failure of database services, misuse of data, Performance degradations etc. Database security measure such as continuous database activity monitoring network traffic or local database, access control, Auditing, authentication, Encryption, Integrity controls, Backups etc. can be used to provides database security.

Network Security Layer:

Network security is to protect [10] the networking system as a whole and sustain its capability to provide connectivity between communicating entities. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network not only means internet but it is collection of different types of networks both private and public. For network security every network resource is given a unique name and corresponding password. Authentication like password, finger print or retinal scan is the first step to network security, next step that can be used is a firewall which will restrict the users to access network services as per the access policies. After this Antivirus software can be used to prevent malware which the firewall may not be able to detect. Communication through network can be encrypted to maintain security. Another method called Honey pots is tools that are deployed in network for investigation and used as early warning tools to explore new exploitation technique along with many other benefits such as misguiding the attacker wasting his time and energy on different server decoy. Honey net is a network of honey pot which is set up with intentional vulnerabilities so that network security can be better implemented by studying attacker's intentions and attacking methods.

The Wi-Fi or wireless network is gaining popularity now days. Wi-Fi threats such as Identity Theft (MAC spoofing), Man-in-middle attacks, Denial of service attack, network Injection etc. are major threats which are increasing. Wireless security is protecting the computer and network resources from unauthorized access. 3333

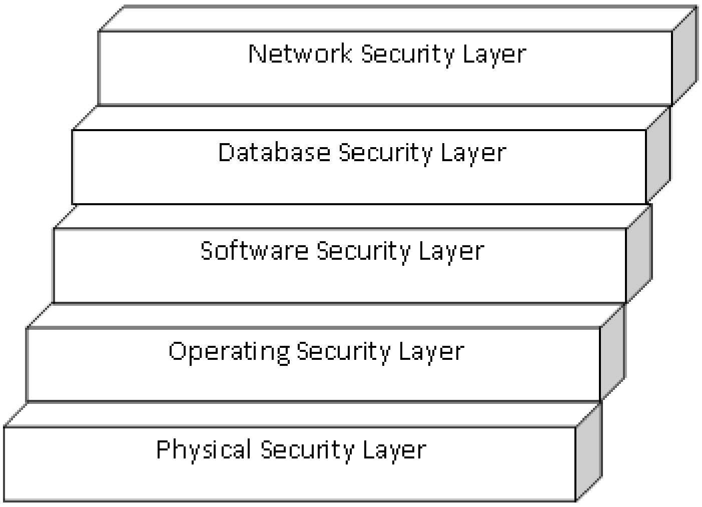


Fig: 4.5 Cyber Security Layer for Cyber Cafe

4.2.4 Cyber Crime, Attack Methodology and Impact

A crime committed or facilitated via the Internet is a Cyber-crime. Cyber-crime is any criminal activity involving computers and networks. The cyber attackers have different motives behind cyber-attack such as sheer thrill, disgruntled employees who are dissatisfied with work environment or are jealous of their colleagues, cyber terrorist who make use of extreme religious or political reasons, theft of sensitive information, disruption of service and illegal access to or use of resources. Cyber-crime affects confidentiality, integrity and availability of computer data. Like physical crimes internet crimes are equivalently dangerous and can lead to serious victimization. Cyber-crimes cannot be considered into single group. Their classification is done depending upon loss of integrity, confidentiality and availability along with the effect it causes to the victim.

The common attacks are phishing and pharming, skimming attack, dictionary attack, Denial of service (DoS) attack, Password-guessing attack and attacks caused by malware.

Malware is a category of malicious code that includes Viruses, Worms, and Trojan and Bots. Malware or malicious code (malcode) is short for malicious [18] software. It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks. Some malware are activated by human intervention and some are spread automatically without human intervention. Malware finds vulnerabilities and exploit them and enter into the system to harm the system. Virus a malware can replicate themselves.

The difference is that a worm operates more or less independently of other files, whereas a virus depends on a host program to spread itself. A virus attaches itself to an executable file or program and while a worm is typically a standalone program. A virus infects a file and uses it as a host from which to infect other files while a worm spreads from one computer to another. Most of the todays viruses propagate at an extra ordinary speed through the network without the intervention of human even before the administrator could be alerted to take remedial action.

4.2.4.1 Types of Cyber Crimes:

Different types of Cyber-Cyber Cafe-crime along with legal measures against them are described in IT Act 2000 amendments. Every day new Cyber-crimes takes place since technology is growing faster and so are the ill intentions of the cyber criminals.

Following are some of the cyber-crimes along with their legal measures as per sections relevant in IT Act 2000 and its amendment.

Cyber Stalking: The crime conducted using internet for communication as email or instant messaging- chat group for following and harassing a person is called cyber stalking. Cyber stalker remains anonymous on the internet. For such crimes IT-Act 43 & 66 is put and punishment of three years with fine is imposed.

Intellectual Property Crime: The crime conducted by manufacturing, distribution, or tampering source code and sale of product is called Intellectual Property Crime. For such crimes IT-Act 43, 65 & 66 is put and punishment of three years with fine is imposed.

Salami Attack (Theft of data manipulating banking account): The cyber-crime conducted by means of unauthorized access to victims account for financial gains. This is achieved by the offender by accessing source code of software application or database. Salami attack is a type of crime in which series of minor attack, results in major attack. For such crimes IT-Act 43 & 66 is put and punishment of three years with fine is imposed.

Email Bombing: In this type of crime the victims accounts are flooded with bulk emails with intentions such as the victim will not be able to read important messages. This act is conducted by making use of different automated tools. For such crimes IT-Act 43 & 66 is put and punishment of three years with fine is imposed.

Phishing: The offender tries to acquire personal information of the victim such as password, credit card details with the intention of stealing money. For such crimes IT-Act 43, 66 and 66c is applied and punishment of three years with fine is imposed. In such cases it is required to take down the system immediately and provide strong authentication mechanism.

Personal data Theft: Stealing of personal information**,** email accounts, bank account information with the intention of financial fraud or harassing the victim is called personal data theft. For such crimes IT-Act 43,43A &72A is applied and punishment of three years with fine is imposed.

Identity Theft: In this type of crime stealing of cyber space information of a victim by hacking or using phishing techniques is done. For such crimes IT-Act 43 is applied and punishment of three years with fine is imposed. Securing computers and safeguarding of personal information should be done to prevent such crimes.

Spoofing: This type of crime is conducted by making use of manipulative tools and techniques for stealing and forging victim's credentials. For such crimes IT-Act 43 & 66 is applied and punishment of three years with fine is imposed. Anti-spoofing measures should be used.

Data Theft: By making use of malicious code computer systems are hacked for stealing the data. Securing the software for preventing data leak must be done .For data theft IT-Act 43, 43A, 65, 66 and 72 is applied and compensation with punishment of three years with fine is imposed.

Worms, Trojans, and Horses & Virus: Malicious codes are used for attacking the victim data or harass the victim. This is done by installing and propagating malicious code. For such crimes IT-Act 43 and 66 are applied and compensation with punishment of three years with fine is imposed.

DOS, DDOS, and Denial of Service: In this type of crime thousands and millions of systems are used to generate traffic. Due to such crime the victim is not able to access the main mail or main services that he need. Such acts are called Denial of service attack. For such crimes IT-Act 43, 66, 66F are applied and compensation with punishment of three years with fine is imposed.

Web Defacing: In such types of crimes the websites are manipulated by various tools and techniques and harass the victims. The websites should be secured by security mechanism and thoroughly checked for loopholes before hosting. For such crimes IT-Act 43, 66 are applied and compensation with punishment of three years with fine is imposed.

Spam Spoofing: In such type of crime unsolicited emails are sent by making use of different techniques either manually or through automated tool. Anti-spoofing or anti spam software's should be deployed at email gateways. For such crimes IT-Act 43, 66 A, 66D are applied and compensation with punishment of three years with fine is imposed.

Publishing or transmitting obscene material: Transmission or publishing of obscene content over electronic media, like networking sites or websites is a crime. In such crimes the websites are removed or the obscene material is taken down. For such crimes IT-Act 67 is applied and compensation with punishment of three years with fine is imposed.

Pornography& Child Pornography: In such type of crimes pornographic material containing sexual explicit act are transmitted. Immediate taking down of pornographic material and corresponding website is done. For such crimes IT-Act 67A and 67B respectively are applied and compensation with punishment of three years with fine is imposed.

Video Voyeurism and Violation Privacy: Transmitting of personal or private video on internet and mobiles is considered crime. For such crimes IT-Act 67E is applied and compensation with punishment of three years with fine is imposed.

Offensive Message: In this type of crime transmitting or communicating in offensive language is done using electronic media. In this type of crimes IT-Act 66A is applied and compensation with punishment of three years with fine is imposed. Awareness among users should be improved to make use of safe internet practices.

Hacking Protected Systems: The offenders make use of various automated tool to hack information infrastructure for such crimes. In this type of crimes IT-Act 70 are applied and compensation with punishment of ten years with fine is imposed.

4.3 Vulnerabilities, Threats and Attacks Overview

When discussing network security, the three common terms used are as follows:

Vulnerability - A weakness in technology, configuration or hardware is termed as vulnerability. Hardware may include servers, UTM or other security devices, hubs and switches, routers and other network components.

■ Threat – Attackers always try to search for loopholes or vulnerabilities and take advantage of it. This is called Threat.

■ Attacks – The attackers use a variety of tools and techniques to attack the vulnerability. The network devices such as the routers or security devices are attacked by attackers.

Vulnerabilities exist in every network and they are considered as favorite spots for threats. The vulnerabilities are of different types such as technology weakness, configuration weakness or security policy weakness.

- Technology weaknesses: This weakness can be loopholes in software or protocols or operating systems. It can also be in firmware software weakness.
- Configuration weaknesses: Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate [11].
- Security policy weaknesses: Security policy weaknesses can create unforeseen security threats. The network can pose security risks to the network if users do not follow the security policy.

There are four primary classes of threats to network security:

- Unstructured threats— these types of threats are from attackers who are inexperienced and make use of available automated tools and techniques.
- Structured threats- These types of threats are from experienced types of attackers who are compatible with technology. These people know how to make use of vulnerabilities and exploit it for their benefits.
- External threats- These threats are from attackers who belong outside the organizations.
- Internal threats- These threats are from individuals who belongs to the organization and has access to the network

4.4 Need of Cyber Security in Cyber Cafe

Cyber security plays a vital role for Cyber Cafe. Internet Cafe is presently the common and simplest gateway to reach entire world. Internet has become a very useful medium for business of different patronage from clients of different classes or race. But along with these there is also increase in the criminal activity on internet with criminal intentions for which Cyber Cafe are the most favorite place that is used by attackers. Internet cafe being public place there is a lot of possibility that privacy can be breached. The owners and visitors of Cyber Cafe face serious cyber security challenges on the internet. Security and privacy is not just about those watching the PC that visitors use, it may even be done electronically using key loggers and screen grabbers. A Key logger [8] is a program that monitors the users behavior and activities on computer and recording it like which keys are pressed, which applications are used, which websites were visited etc. and storing the data on the hard disk or to a website designed for such purpose. Screen grabbers are like key loggers but they grab the content on the display. Other than these phishing, malwares, hacking are some other cyber-attacks that create problems for Cyber Cafe visitors. Along with these Wi-Fi hotspots is gaining popularity. For these and many such problems cyber security plays a very important role not only in Cyber Cafe but at all public places such as restaurant, airports, shops, coffee shops, etc. In an intentional Wi-Fi attack a malicious user disrupts Wi-Fi communications through use of a normal PC and software or a custom jammer. This type of attack can both cause Denial of Service (DoS) attack, and breaches that provide illicit access to the network.

Other Wi-Fi security threats are Protocol level attacks, that attempt to enter Wi-Fi data security include rogue access point, authentication attacks, evil twin access points, man-in—the-middle attacks etc. Thus Wireless or wired network there is always a possibility of being into danger through cyber-attack. If proper cyber security is not implemented then there are more chances of getting hampered.

Also due to these cyber-attacks the Cyber Cafe reputation is getting hampered and visitors fear to visit Cyber Cafe. The Cyber Cafe business is facing problems and the owners strongly feel that if better cyber security policies and methods are available then Cyber Cafe business can flourish more.

4.5 Role of Government, Cyber Cafe Owners/Owner and Visitors in Management of Cyber Security.

In order to ensure that society continues to enjoy the benefits of Cyber Cafe, the vulnerabilities and risks are to be managed through the cyber security [4] efforts of the stakeholders that own, develop, operate and use the Internet. These stakeholders include government, Internet Service Provider, third party software venders, Cyber Cafe owners and visitors.

- **Role of Government**

  Governments play a major role and are in a position to lead national cyber security efforts that involve stakeholders. The government has substantive measure to counter cyber security threats. Government cyber security roles for Cyber Cafe include

  - **Policy making**: A common policy for Cyber Cafe to implement cyber security. Establish cyber security objectives such as detection and prosecution of Cyber-crime, protection of data etc. Identification of actions to be taken in order the objectives is not achieved. Establishment of incident response teams such as Cyber-crime cell, Building awareness among citizens and Allocating roles and responsibilities to Cyber Cafe owners, visitors and police.
  - **Legal Measures**: For effective cyber security at Cyber Cafe needs establishment of cyber security infrastructure such as Cyber-crime cell, cyber forensic lab, and review are taken, and if necessary amendment in rules and regulation are done.

- **Government cyber security authorities and Cyber Cafe association or owners coordination**: The coordination and collaboration between Government stakeholders and Cyber Cafe owners is extremely important for successful cyber security implementation. Meetings between Cyber Cafe association and police for creating awareness and finding solution to problems of Cyber Cafe owners.

  There are various stakeholder agencies of government like National Information Board (NIB), National Crisis Management Committee (NCMC),National Security Council Secretariat(NSCS), Ministry of Home Affairs, Ministry of defense, Department of Information Technology(DIT),Department of Telecommunications(DoT),National Cyber Response Centre, Indian Computer Response Centre, Indian Response Team(CERT-In) National Information Infrastructure Protection Centre(NIIPC), National Disaster Management of Authority (NDMA), Standardization, Testing and Quality Certification (STQC) Directorate, Sectorial CERTs. Annexure - II
- **Incident management and cyber security readiness assessment:** The most important part of cyber security is to detect attacks, identify the threats, analyze the impact and provide a suitable response. The response should include vulnerability assessment and management along with suitable response option that can be taken. Computer Emergency team (CERT) have been established at the national level which will provide timely information about latest threats and assistance in response to incidents when needed.
- **Building cyber security awareness:** Cyber security can be improved if the people in the society form a environment of cyber security. This can be done by improving awareness about cyber security among people. Awareness can be improved through cyber security training, interactive cyber security websites, and making mandatory for widely accepted security certifications along with encouragement for academia to provide

    cyber security training to students to meet the increasing demands of both the public and the private sector in the field.

  - **Development of cyber security framework for Cyber Cafe with public**: Development of framework which will allow government, Cyber Cafe owners, visitors, Internet Service Provider to work together to develop and implement measures that incorporate technical(e.g. standards), procedural(e.g. guidelines, standards or mandatory regulations) and personnel(e.g. best practices) safeguard. The frame work development include implementation and adoption of international standards related to cyber security (e.g. ISO 27001)

- **Role of Cyber Cafe Owners/Owners**: The Owners plays a major role for implementation of cyber security in Cyber Cafe. The owners follows the rules and regulations for cyber security as put forth by the government. Owners need to keep themselves updated with latest cyber security trends or alerts. They should have knowledge to take necessary action in case a cyber-attack is under way or Cyber-crime has taken place. The owners should cooperate with the government cyber security personnel and work in collaboration with them to implement cyber security. Cyber Cafe owners should protect the visitor’s privacy by taking precautionary measures such as installing reliable antivirus software, antispyware software following rules and regulations, displaying boards of rules of Cyber Cafe etc.
- **Role of Visitors:** Visitors visiting the Cyber Cafe should follow rules and regulations of the Cyber Cafe. They should be aware about cyber security and Cyber-crime. Necessary precautions such as checking updated antivirus, different passwords for different websites, keeping personal and official accounts different, using private browser, making necessary security settings such as switch off the auto save part for password and username, disabling the file sharing option ,being attentive in cafe that nobody watches your actions, not leaving the computer unattended etc. Visitors should protect their privacy first by

taking necessary cyber security steps. In case they become victim of Cyber-crime they should know where to report and what further steps they should take to avoid further problems.

- **Role of ISP:** Internet Service provider plays an important role in transmitting the third party content on internet. These are the stakeholders who are responsible to take care about the content on the internet and prevent any unlawful content, as per Ministry of communication and Information Technology Department of Electronics and Information Technology. ISP should cooperate with government to provide details required by the government in case a Cyber-crime occur.

4.6 Challenges for Cyber Security Management for Cyber Cafe in India

Cyber Cafe stakeholders face many challenges for cyber security management in Cyber Cafe. According to National Crime Bureau (NCRB) there were a total of 426 arrests under IT Act 2013. The first and foremost is the laws for Cyber Cafe are not clearly defined. The laws need to be revised on regular time interval as technology changes at a rapid speed. For the current laws from that are put forth by the government in Information Technology (Guidelines for Cyber Cafe) Rules 2011 that were notified by the Central Government in the Gazette of India vide Notification GSR 315(E) on 11 April 2011 (“Cyber Café Rules”)following lacunas can be see:

- Rule 2(1)(c) of the Cyber Cafe Rules defines a Cyber Cafe in accordance with the definition provided in section 2(1)(na) of the IT Act as follows:

  “Cyber Cafe” means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public”

  According to this definition all the places such as airports, institute, restaurants, Indian Railways, Libraries, organizations and other establishments which provide internet service are Cyber Cafe. The definition of “Cyber Cafe” should be such as it includes only commercial establishments that primarily offer internet services to the general public for a fee.

- Rule 3 - Agency for Registration of Cyber Cafes

  All Cyber Cafes across India are already registered under applicable local and municipal laws such as the relevant State Shops and Establishments Acts and the relevant Police Acts that provide detailed information to enable the relevant government to regulate Cyber Cafes. So there is no need for one more registration agency for Cyber Cafe registration which will actually increase the burden of Cyber Cafe owners.

- Rule 4 - Identification of User

  Identification of users by making use of visitors credential may result in identity theft. Even Reserve bank of India discourages credit cards or debit cards to be used as identification proofs.

- Rule 4(2) of the Cyber Cafe Rules compels the storage of photographs and other person

  This rule may give rise to identity theft and other offences. This rule requires Storing user information for the purposes of law enforcement, it does not prescribe the standards of security, confidentiality and privacy that should govern the storage of photographs and other personal information by Cyber Cafes. Without such a prescription, Cyber Cafes will simply store photographs of users, including minors and women, and important personal information that can be misused, such as passport copies, in a file with no security. This is unacceptable.

- Sub-rule (3) of rule 4 allows Cyber Cafe users to be photographed

  This rule invades the individual privacy rights of users. Besides rule4 (1) all contain a photograph of their owner so there is no need of further photography and even the owners are burden who will be required to store two sets of photographs of users.

- Sub-rue (4) of rule 4 reads as follows:

"Rule (4) A minor without photo Identity card shall be accompanied by an adult with any of the documents as required under sub-rule (1)."

This rule discourages education and awareness through internet access to minors. Most minors do not possess photographic identity documents and rule 4(4) will, if implemented, result in internet access being taken away from minors.

- Rule 5(3) of the Cyber Cafe Rules states:

  "(3) Cyber Cafe shall prepare a monthly report of the log register showing date- wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by the 5th day of next month."

  This rule may violate the individual right to privacy since protective provision to safeguard individual internet usage which is required to be maintained are not there. There may be instances where public interest may be served by monitoring the internet history of specific individuals.

There are still many problems faced by the cyber owners due to the poor draft of rules and regulations. Due to these strict rules and regulations visitors hesitate to visit the Cyber Cafe. This has resulted in loss of business of Cyber Cafe. Thus the laws should be updated at a faster rate.

The owners face difficulties to consider all angles of cyber security in Internet cafes such as Physical Security, Operational level security, Application level Security and Network Level security. No special provision or guidance for wireless network is mentioned in the law. Wireless network is now a days becoming popular so there is a need to focus on wireless cyber security. Awareness among people must be made about cyber security. In case any Cyber-crime is under way or has taken place the owners only know that they have to communicate to the police but they do not have sufficient knowledge how to handle the situation or what steps to be taken. The owners are not trained for this purpose neither they keep themselves alert with the current Cyber-crime or attacks and recent updates in the ICT world. Due to financial problems some of them are not able to update latest software such as operating system, antivirus, antispyware etc. which may hamper cyber security. The police authority approaching the Cyber Cafe owners for verification should have sufficient knowledge about cyber security management otherwise there is unnecessary harassment to the owners. The owners should not be held responsible for any crime that takes place at his Cyber Cafe. Instead government initiative of centralized database for visitors should be made and all logs related to visitor’s activity can be stored so that monitoring of the activity will be easily for the government instead of the owners keeping record of it.

References

Sr. No	References
1	3 pillars of industrial cyber security - Article published by - Dennis Brandl 07/16/2012 - http://www.csemag.com/single-article/3-pillars-of-industrial-cyber-security/ae9f214bcd0f00fba81c041826a94d34.html 8/3/2012
2	Anikar M. Haseloff - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 - http://ci-journal.net/index.php/ciej/article/view/226/181 - 12/5/2014
3	Application Security article- http://searchsoftwarequality.techtarget.com/definition/application-security 5/7/2012
4	CIS Para-wise Comments on Cyber Café Rules - 2011 - http://cis-india.org/internet-governance/front-page/blog/cyber-cafe-rules -13/12/2012
5	Computer security article - https://en.wikipedia.org/wiki/Computer_security - 8/8/2014
6	Cyber Security and IT Security - http://security.stackexchange.com/questions/57976/nowadays-what-is-the-difference-between-cyber-security-and-it-security - 5/7/2013
7	Information security article- https://en.wikipedia.org/wiki/Information_security -4/7/2013
8	Keyloggers - Article Published By Nikolay Grebennikov on March 29, 2007 - https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1 8/8/2013
9	Larss Magnus Frodigh, Per Johansson and Peter -Ericsson - "Wireless ad hoc networking—The art of networking without a network"- http://www.ericsson.com/ericsson/corpinfo/publications/review/2000_04/files/2000046.pdf - 7/3/2013
10	Network and Security - http://www.techsoupforlibraries.org/book/export/html/592 5/7/2013
11	Network Security -Book Published by Perason Education- Antoon -W-Rufi- 2007 ISBN- 81-317-0892-6 8/8/2013
12	Otusile Oluwabukola , S. A. Idowu and Ajayi Adebowale-"Overview of Database Architecture and Security Measures – Attacks and Control Methods"- - Asian Journal of Computer and Information Systems (ISSN: 2321 – 5658) Volume 02 – Issue 02, April 2014 - 2/7/2014
13	Reinventing Cyber Cafes- http://www.ccaoi.in/UI/links/articals.php?Id=4&action=view 7/7/2013
14	Report on Compilation of Existing Cybersecurity and Information Security Related Definitions- October 2014 - Tim Maurer & Robert Morgus- https://www.newamerica.org/downloads/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions.pdf 8/7/2013

15 Report on Guide for Developing Security -Plans for Federal Information Systems - Marianne Swanson Joan Hash Pauline Bowen http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf 7/7/2014

16 Safeguarding your Tecnology(Book)- Written by - Tom Szuba- September - 1998 - https://nces.ed.gov/pubs98/safetech/chapter5.asp 8/8/2014

17 System software -https://en.wikipedia.org/wiki/System_software 9/9/2013

18 Viruses, Worms, Trojans, and Bots - http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html 8/8/2014

CHAPTER 5

DATA ANALYSIS AND INTERPRETATION

5.1 Introduction

The study is related to the Cyber security management for Cyber Cafe in Pune city. The researcher has used survey based research methodology to carry out this research. The researcher has tested positively the hypotheses of this research study, with the help of primary and secondary data. For the purpose of the study, samples are divided into two parts. **Part I** is about Owners of Cyber Cafe and **Part II** is about Visitors of Cyber Cafe who avail Cyber Cafe services. The researcher has selected two samples viz. Owners and Visitors of Cyber Cafe and collected data from them. The first sample consists of 134 Cyber Cafe Owners of Pune city from 4 zones including 14 ward offices. The second sample has 384 Cyber Cafe Visitors from registered Cyber Cafes. They are shown in Table No.5.1

Table No. 5.1: Selection of Sample

Sample Type	Constituents	Number of Sample points in the sample from 14 Ward offices
1	Owners	134
2	Visitors	384

The data is collected through interviews and questionnaires and compiled in 29 tables for Cyber Cafe Owners and for Cyber Cafe Visitors. Statistical parameters and graphics have been used wherever necessary and useful. The data analysis is grouped in 2 parts as given in the next paragraphs.

Presentation and Analysis of Data I: Pune Cyber Cafe Owners

In Part I, the primary data about 134 Cyber Cafe Owners from 14 ward offices of Pune city has been collected by the researcher (Para 2.7.1 D).An analysis is carried out in four broad headings as follows:

1. General background of Cyber Cafe Owners with respect to their Education, Computer Background and Problems faced for running Cyber Cafe.
2. Awareness and status of Cyber Cafe Security Management and Cyber-crime knowledge.
3. Rules & Regulations of Cyber security in Cyber Cafe and their impact on Cyber Cafe Owners.
4. Costs Benefit Analysis (CBA) for Cyber Cafe from Owners perspective.
5. Design Cyber Security framework for Cyber Cafe.

Presentation and Analysis of Data II: Cyber Cafe Visitors

In Part II, the primary data has been collected by the researcher with respect to 384 Visitors from Pune (Para 2.7.1 D). For the purpose of the study, the researcher has selected Cyber Cafe Visitors from Cyber Cafe of 14 ward offices of Pune city. The Visitors' analysis is carried out in three broad headings and is as follows:

1. General background of the Visitors with respect to their gender, education and Cyber Cafe usage.
2. Awareness of Cyber Cafe Visitors regarding Cyber Security Management.
3. Impact of Cyber security rules and regulations on the usage of Cyber Cafe services on Cyber Cafe Visitors.

5.2 Pilot Study

The researcher has conducted pilot survey randomly to test the questionnaire. To know the consistency of questionnaire to be administered for the research, researcher has applied the Cronbach’s Alpha reliability test. Initially the questionnaire was circulated to 10 Cyber Cafe Owners & 22 Cyber Cafe Visitors and reliability test was conducted.

The result of pilot survey about Cyber Cafe Owners is given in following Table No. 5.2 and about Cyber Cafe Visitor in Table No. 5.3 respectively.

Table No. 5.2: Reliability Statistics of Owners

		No. of Respondents	%	Cronbach's Alpha	No. of Items
Cases	Valid	10	100.0	.958	152
	Excluded[a]	0	0.0		
	Total	10	100.0		

a. List wise deletion based on all variables in the procedure

For checking the reliability of the Owners questionnaire Cronbach's Alpha test is used. 152 items are considered for Cronbach’s Alpha test. As per the Table No. 5.2 reliability statistics of Owners Questionnaire is 0.958. It means 95 percent respondents understood the questionnaire. Thus researcher concludes that reliability of the questionnaire is satisfactory so same questionnaire can be administered for the further research.

Table No. 5.3: Reliability Statistics Visitors

		No. of Respondents	%	Cronbach's Alpha	No. of Items
Cases	Valid	22	100.0	0.907	85
	Excluded[a]	0	0.0		
	Total	22	100.0		

a. Listwise deletion based on all variables in the procedure

For checking the reliability of the Visitors questionnaire Cronbach's Alpha test is used. 85 items are considered for Cronbach’s Alpha test. As per the Table No. 5.3 reliability statistics of Visitors Questionnaire is 0.907. It means 90 percent respondents understood the questionnaire. Thus researcher concludes that reliability of the questionnaire is satisfactory so same questionnaire can be administered for the further research

5.3 Presentation and Analysis of Data I: Pune Cyber Cafe

Introduction

Cyber Cafes play a significantly different role in India, compared to the role they play in the most developed countries. Whereas in developed countries, they are just an additional access point for people who already have access somewhere else, they seem to be highly important for the middle class in India. An Internet Cafe or Cyber Cafe is a place which provides internet access to the public by charging fees. It includes any commercial establishment or Internet kiosk, the objective of which is to make Internet services available to the general public. The fee for using a computer is usually charged as a time-based rate. Cyber Cafe is considered to be a “Place of Public Amusement as defined under section 2 (9) of the Bombay Police Act, 1951” (Act XXII of 1951).Cyber Cafe license is allotted only after checking if all norms provided by the government are fulfilled. A Cyber Cafe Owners is one who runs the Cyber Cafe and takes care about the Cyber security management while following the rules and regulations put down by the government.

5.4 General Background of Cyber Cafe Owners

Pune, the Oxford of the East and hub of Information Technology is also a historical city in India with a glorious past, an innovative present and a promising future. For administrative purposes Pune city is divided into four zones with 14 ward offices which include 144 wards.

As a major venue of public access to Information and Communication Technologies (ICT), Cyber Cafes in India have been contributing to the increase of ICT penetration, especially Internet penetration for the last decades. Although Internet is a vital source of information, the misuse and the Cyber-crime have also increased. Government has taken efforts to make Cyber-crime law stringent. Cyber Cafe Owners follows these government laid rules and regulations to run the Cyber Cafe so that Cyber-crimes are reduced.

To know about the Cyber Cafe Owners of Pune city one needs to study the general background which covers their education and Cyber security knowledge. Such background is essential to ascertain their knowledge about computer literacy, internet literacy and awareness of the Cyber security management system and their rules and regulation.

5.4.1 Background of Respondents according to their Education and ICT Knowledge

In today's IT world citizens should be educated and should have an adequate knowledge of computers, internet as well as Cyber security. These are important factors related to the Cyber security management by Cyber Cafe Owners. Cyber security can be implemented by Cyber Café Owners only if they have computer literacy and are aware about Cyber security. Computer Literacy and Cyber security is one of the key socio-economic progress measures of modern society and an important aspect of Indian society. According to the latest Indian Population Census 2011, the average literacy rate of Pune city is 91.61 percent and it is high as compared to State and National level average literacy rate.

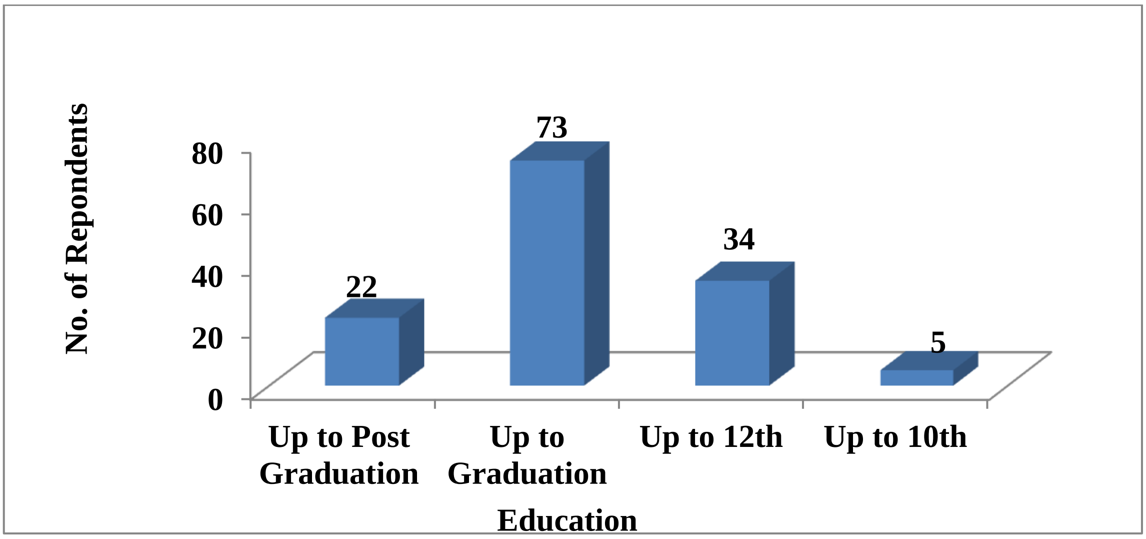
Table No. 5.4 represents the distribution of respondents according to their education. It is seen that a majority of over 54.50 percent respondents are graduates. It is followed by 25.40 percent respondents who have completed their education up to 12th& above degree. A further 16.40 percent respondent has completed their education up to post-graduation. The rest of the 3.70 percent respondents have completed their education up to 10th. The proportion of graduate respondents is higher than post graduates, secondary and higher secondary.

Table No.5.4: Distribution of No. of Respondents according to Education

Education	No. of Respondents
Up to Post Graduation	22 (16.40)
Up to Graduation	73 (54.50)
Up to 12th	34 (25.40)
Up to 10th	5 (3.70)
Total	134 (100.0)

Figures in bracket indicates Percentage

Graph 5.1: Distribution of No. of Respondents according to their Education



As can be seen in Graph 5.1, it is apparent that most of the respondents are graduates followed by higher secondary, post graduates & above and then secondary. It shows that most of the Cyber Cafe Owners are well educated.

5.4.2 Background of Respondents according to their Computer Knowledge

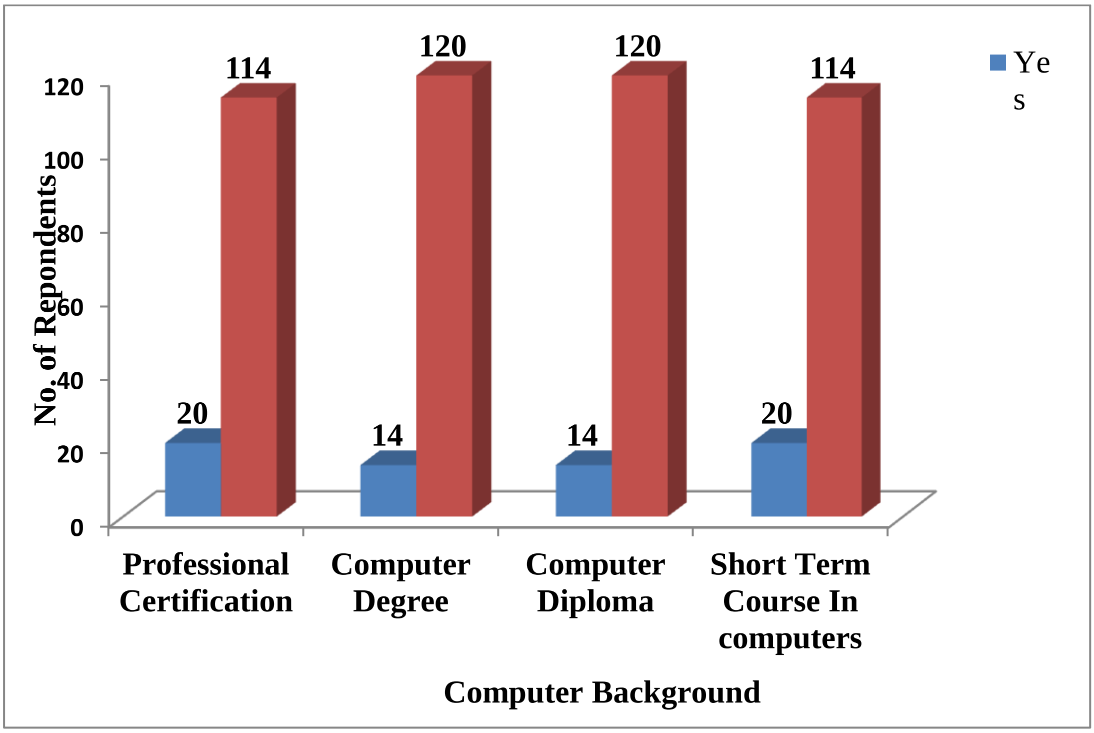
Table No.5.5 represents the distribution of respondents according to their Computer Knowledge. 14.90 percent respondents have done professional certification or short term course in computers. The total percentage of the respondent who have done computer degree or computer diploma is 10.40 percent.

Table No.5.5: Distribution of No. of Respondents according to their Computer Knowledge

Computer Background	No. of Respondents		Total
	Yes	No	
Professional Certification	20 (14.9)	114 (85.1)	134 (100)
Computer Degree	14 (10.4)	120 (89.6)	134 (100)
Computer Diploma	14 (10.4)	120 (89.6)	134 (100)
Short Term Course In computers	20 (14.9)	114 (85.1)	134 (100)
Total	68	468	
Average Percentage	(12.65)	(87.35)	

Figures in bracket indicates Percentages

Graph 5.2: Distribution of No. of Respondents according to their Computer Background



As can be observed from Graph 5.2, Very less respondents have done professional certification and short term computer course as their computer background followed by computer diploma and computer degree. Respondents are not much computer literate. Overall only 12.65 percent respondents are computer literate out of total sample. Rest they fall in computer illiteracy category. Still they operate the Cyber Cafe based on practical experience.

5.4.3 Problems Faced By Cyber Cafe Owners While Running Cyber Cafe Based On Rank

Cyber Cafe Owners face many problems while implementing the rules and regulations for Cyber Cafe obligatory by the government. An attempt has been made to assess the problems faced by the Cyber Cafe Owners by noting the observations. Table No. 5.6 shows the various parameters of problems faced by Cyber Cafe Owners and their rank order. To meet the objective of the study, a questionnaire has been designed by using various parameters which define the various problem factors faced by the Cyber Cafe Owners. It is observed that for each parameter the average scale is in between 1 to 5 that is in between strongly disagree to strongly agree. In fact all the values are above 3.5 which mean that with respect to all the parameters much approval is observed. In a 5-point Likert scale, categories like strongly agree, agree, neutral, disagree and strongly disagree clubbed into three categories. The reason for using Likert scale is that the responses by the respondents should not become monotonous while answering the questions. Hence researcher has also applied 5-point Likert scale and calculates weighted average value. There is very less difference between the comparative value of traditional average value and 5-point Likert scale value.

It is seen that the highest average value is 4.1 for the factor ‘Reputation Hampered’ followed by ‘High Maintenance Cost’ with average weight of 4.08 and ‘lack of resources to assist in Cyber-crime attack’ and ‘Lack of indicators attacks underway’ which is having average weight 3.91. The average weight for the factor ‘Lack of established resources to know about Cyber security updates' is 3.86 followed by 'Lack of knowledge of security maintenance' having average weight 3.8.

It is clear from the average weight values that respondents face many problems while running the Cyber Cafe. While implementing rules and regulations, government has to assist respondents in case of Cyber-crime. Suitable training must be given to Owners so that they will be aware of new Cyber-crime, new technologies, and resources from where they can find information to improve and maintain security.

Table No.5.6 also shows the ranks of each parameter used for assessment of the problems faced by the respondents. Based on the primary data respondents feel that due to the rules and regulations their business reputation is hampered. This parameter ranks *first* with a weightage of 65.60 percent, followed by High maintenance cost which is ranked *second* with a weightage of 67.18 percent. Some respondents feel that there is lack of resources to assist in Cyber-crime attack which is the *third* parameter. This parameter has a weight of 71.70 percent. If the government provide resources to handle the Cyber-crime attack then it would be easier for the respondents to handle it. 73.90 percent respondents feel that there is lack of indicators to notify that a Cyber-crime attack is under way which is ranked *fourth*. 66.40 percent respondents feel that there is lack of resources to know about Cyber security updates which is ranked fifth. Finally 59.70 percent respondents which is ranked sixth and is for lack of knowledge of security maintenance.

It is seen that 67.40 percent respondents agree that there are problems faced by them. According to this it is clear that government should take initiative to solve Cyber Cafe Owners problems.

Table No.5.6: Problems Faced by Cyber Cafe Owners while Running Cyber Cafe based on Rank

Problems Faced	**SD**	**D**	**N**	**A**	**SA**	**Total**	**Wt. Avg**	**Wt. Avg (Likert Scale)**	**Rank Order**
Reputation Hampered	6 (4.50)	2 (1.50)	38 (28.40)	14 (10.4)	74 (55.2)	134	4.1	4.31	1
High Maintenance Cost	8 (5.9)	2 (1.5)	34 (25.40)	17 (12.70)	73 (54.48)	134	4.08	4.35	2
Lack of resources to assist in Cybercrime attack	15 (11.20)	0	23 (17.20)	40 (29.90)	56 (41.80)	134	3.91	4.35	3
Lack of Indicators attacks underway	10 (7.50)	3 (2.20)	22 (16.40)	41 (30.60)	58 (43.30)	134	3.91	4.34	4
Lack of established resources to know about Cyber security updates	9 (6.70)	0	36 (26.90)	44 (32.80)	45 (33.60)	134	3.86	4.13	5
Lack of Knowledge of security Maintenance	12 (9)	4 (3)	38 (28.40)	24 (17.90)	56 (41.80)	134	3.8	4.22	6
Total	60	9	191	180	362				
Average Percentage	**7.46**	**1.37**	**23.77**	**22.37**	**45.03**				

Figures in bracket indicates Percentages

(Note: Average scale on 1 to 5 (where Strongly Disagree (SD) =1; Disagree (D) =2; Neutral (N) =3; Agree (A) =4; Strongly Agree (SA) = 5))

5.4.4 Internet Connection Type used in Cyber Cafe

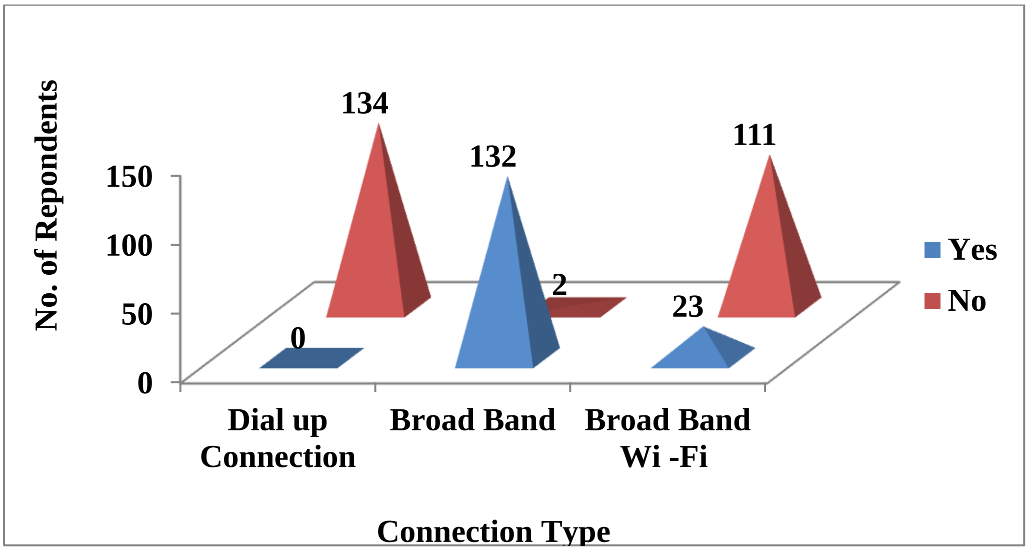
There are many types of Internet connection that can be used in Cyber Cafe like Dial Up connection, Broad Band connection and Hotspot also called Wi-Fi. According to the Table No. 5.7, it is clear that most of the respondents have Broad Band connection type with 98.50 percent. Only 17.16 percent respondents use broad band Wi-Fi and nobody use dial up connection. Also it was observed that leased line was not used by any respondent.

Table No.5.7: Connection Type used in Cyber Cafe

Sr. No.	Connection Type	No. of Respondents		Total
		Yes	No	
1	Dial up Connection	0	134 (100)	134 (100)
2	Broad Band	132 (98.5)	2 (1.5)	134 (100)
3	Broad Band Wi-Fi	23 (17.16)	111 (82.84)	134 (100)

Figures in bracket indicates Percentages

Graph 5.3: Connection Type used in Cyber Cafe



From the Graph No. 5.3, it is clear that most of the respondent use Broad Band connectivity for Cyber Cafe. Wi-Fi is on increasing demand now a days and during collection of primary data it is observed that many non-registered Cyber Cafe use Wi-Fi.

5.4.5 Awareness of Cybercrime among Cyber Cafe Owners

Cyber-crime is a crime which is done by using a computer. These Cyber-crimes are of many types. Questionnaire includes some types Cyber-crimes to check the awareness about Cyber-crimes of respondents. Table No.5.8 shows that 69.40 percent respondents are aware about Cyber pornography, 59 percent respondents are aware about Intellectual Property crime, 54.50 percent respondents are aware about Money Laundering Evasion, 61.20 percent respondents are aware about Electronic fund transfer, 68.70 percent respondents are aware about hacking, 58.20 percent respondents are aware about Email spoofing followed by 51.50 percent respondents are aware about political crime, 53.70 percent respondents are aware about Electronic Terrorism and 47.80 percent respondents are aware about E-murder.

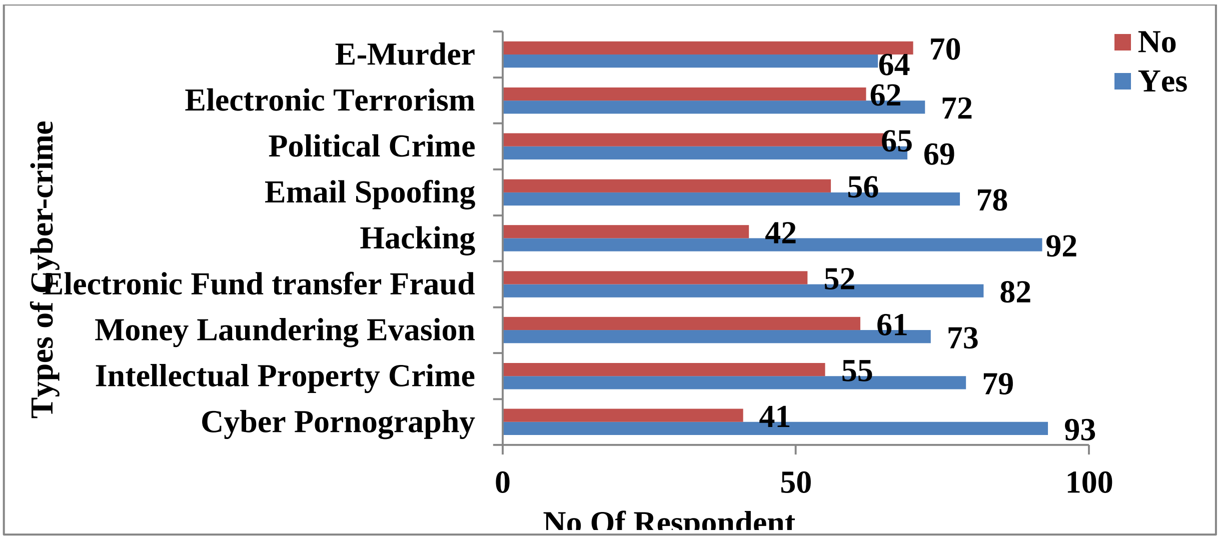
The average awareness about Cyber-crime of respondents was 58.23 percent. It indicates that most of respondents have knowledge about Cyber-crime but still it needs to be improved.

Table No.5.8: Cyber-crime Awareness of Cyber Café Owners

Sr. No	Types of Cyber-crime	No. of Respondents		Total
		Yes	No	
1	Cyber Pornography	93 (69.40)	41 (30.60)	134 (100)
2	Intellectual Property Crime	79 (59.0)	55 (41.0)	134 (100)
3	Money Laundering Evasion	73 (54.5)	61 (45.50)	134 (100)
4	Electronic Fund transfer Fraud	82 (61.20)	52 (38.80)	134 (100)
5	Hacking	92 (68.70)	42 (31.30)	134 (100)
6	Email Spoofing	78 (58.20)	56 (41.80)	134 (100)
7	Political Crime	69 (51.50)	65 (48.50)	134 (100)
8	Electronic Terrorism	72 (53.70)	62 (46.30)	134 (100)
9	E-Murder	64 (47.80)	70 (52.20)	134 (100)
Total		702	504	
Average Percentage		58.23	41.77	

Figures in bracket indicates Percentages

Graph 5.4: Cyber-crime Awareness of Cyber Café Owners



The Graph No. 5.4 clearly shows that most of the respondents are aware about Cyber-crime such as Cyber Pornography, Hacking, Intellectual property crime and many others. This knowledge is important to Owners which help them to prevent Cyber-crime and take necessary actions in case it takes place.

5.4.6 Summary

The majority of Owners are graduates and few of them have completed post graduation degree. It is seen that very less number of Owners have computer background. Different types of problems are faced by Owners while running the Cyber Cafe such as lack of assistance in case a Cyber-crime occurs, High maintenance cost, Lack of indicators in case an attack of Cyber-crime is under way and many others. Most of the Cyber Cafe has Broad Band connection and it is observed by the researcher that most of the non-registered Cyber Cafe has Wi-Fi in there Cafe. Owners are also aware about various types of Cyber-crime like pornography, hacking and many other which a good sign for Cyber security awareness in Owners.

Computer literacy is less which should be improved. Most of the Owners face problems while running the Cyber Cafe. Also the awareness about Cyber-crime is good but still needs to be improved among Owners.

5.5 Awareness and Status of Cyber Cafe Security Management

An attempt was made to meet the objective of the study which is "*To study the awareness of Cyber security management among Owners & Visitors of Cyber Cafe and to study the present Cyber security provided in Cyber Cafes by Owners*." Such an analysis aims to know the awareness of Cyber security management among Cyber Cafe Owners in Pune City. To study the awareness of security management, various parameters are considered for study such as Cyber security techniques used, Cyber security maintenance method and physical security provided.

The internet [4] is expanding at a rapid pace and it has already been a player in the field of government offices, business, economy, entertainment and social groups all over the globe. The rise of internet usage all over the world has unlocked various new businesses, products, and services. The internet is changing and it will continue to do so. The number of internet users is increasing day by day. It has reached 2095 million at the end of 2011, compared to 1,996 million users in the year 2010. The statistics reveal that China has the largest number of users with 513 million and the US is second overall with 245 million. The strongest growth is seen in India which is ranked third where the number of users is 121 million. If Cyber Cafe Owners implement proper Cyber security and are aware about Cyber security management then Cyber-crimes can be avoided.

5.5.1 Cyber Security Level Maintained in Cyber Cafe

Cyber security can be implemented at two levels that is End Level and Gateway Level or Both. Maximum security should be provided by using various Cyber security techniques. The collected primary data from the Cyber Cafe Owners relates to the different Cyber security methods and techniques used at various levels to implement Cyber security management.

From the Table No. 5.9, it is seen that most of the respondents implement Cyber security by self method that is 85.07 percent whereas at the Automated method is 14.93 percent. 30.60 percent respondents' implements cyber security at End Point level, out of which 23.88 percent respondents make use of Self method and 6.72 percent respondents make use of automated method. 66.42 percent respondents implements cyber security at Gateway level, out of which 59.70 percent respondents make use of Self method and 6.72 percent respondents make use of automated method. 2.98 percent respondent's implements cyber security at Both level, out of which 1.49 percent respondents make use of Self method and automated method.

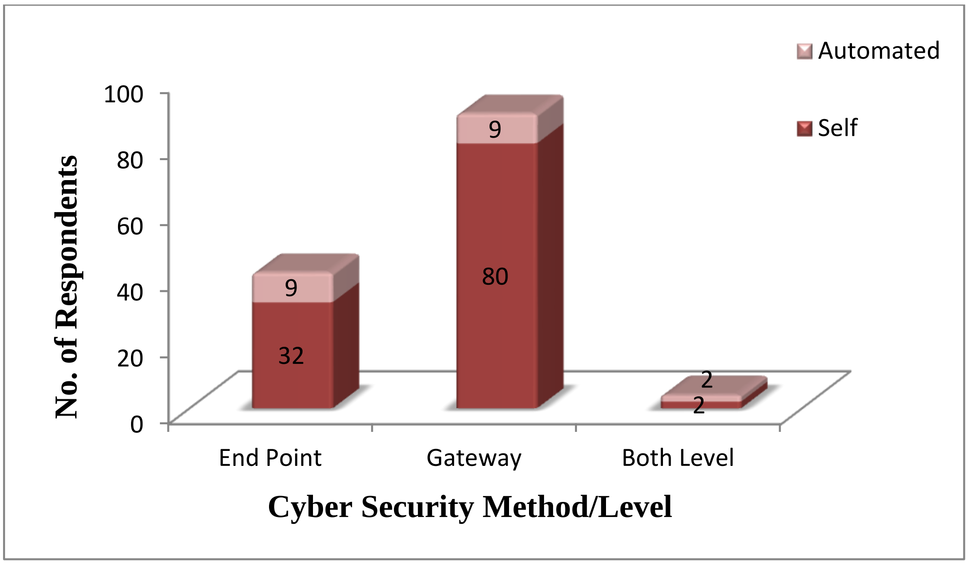
It is seen that most of the respondents implements cyber security at Gateway Level which is good but it should be maintained at both the levels.

Table No.5.9: Cyber Security Method and Level Maintained

Method /Level	End Point	Gateway	Both Level	Total
	Yes	Yes	Yes	
Self	32 (23.88)	80 (59.70)	2 (1.49)	114 (85.07)
Automated	9 (6.72)	9 (6.72)	2 (1.49)	20 (14.93)
Total	41 (30.60)	89(66.42)	4(2.98)	**134** (100)

Figures in bracket indicates Percentages

Graph 5.5: Cyber Security Method and Level Maintained



From the Graph 5.5 it is clear that that most of the respondent maintained Cyber security at gateway level and the cyber security is implemented by them. It is seen that there are few respondents who maintain security at both level. Thus it is clear that respondents are aware about Cyber security implementation at various levels and presently most of them implement Cyber security at Gateway level.

5.5.2 Cyber Security Techniques used in Cyber Cafe

There are various Cyber security techniques that can be used in Cyber Cafe which if implemented properly can avoid Cyber-crimes such as virus dissemination, money laundering, spamming, phishing and many more. From the primary data collected it shows that different Cyber security techniques are used by Owners to implement Cyber Security. Table No.5.10 (A) shows that 96.30 percent respondents used antivirus software as security techniques which are good and necessary followed by 44 percent respondents having Endpoint security software installed and 58.20 percent respondents used antispyware software. 76.90 percent respondents had Firewall settings done which is available default with operating system. 63.40 percent respondents used Network access control so that required access to network can be given. Further 50 percent respondents used control panel access restriction followed by 38.80 percent browser security option restriction. 47.80 percent respondents used physical drive restriction and 46.30 respondents used default security option. Whereas 57.50 percent respondents changed the router username and password frequently and 38.10 percent respondents blocked the setup files and automatic installation of software without Owners concern. 13.40 percent respondents have installed Unified Threat Management Device (UTM) and UTM software which protects from vulnerabilities. 42.50 percent respondents used website keyword blocking mechanism by using antispyware or antivirus software or through service provider by default and are aware about this feature. 26.10 percent respondents used content filter so that crimes such as hatred mail, pornographic website viewing and other crime can be avoided.

It is observed that 49.58 percent respondents are aware about Cyber security techniques to be used to avoid Cyber-crimes and have apparently implemented them in their Cyber Cafe.

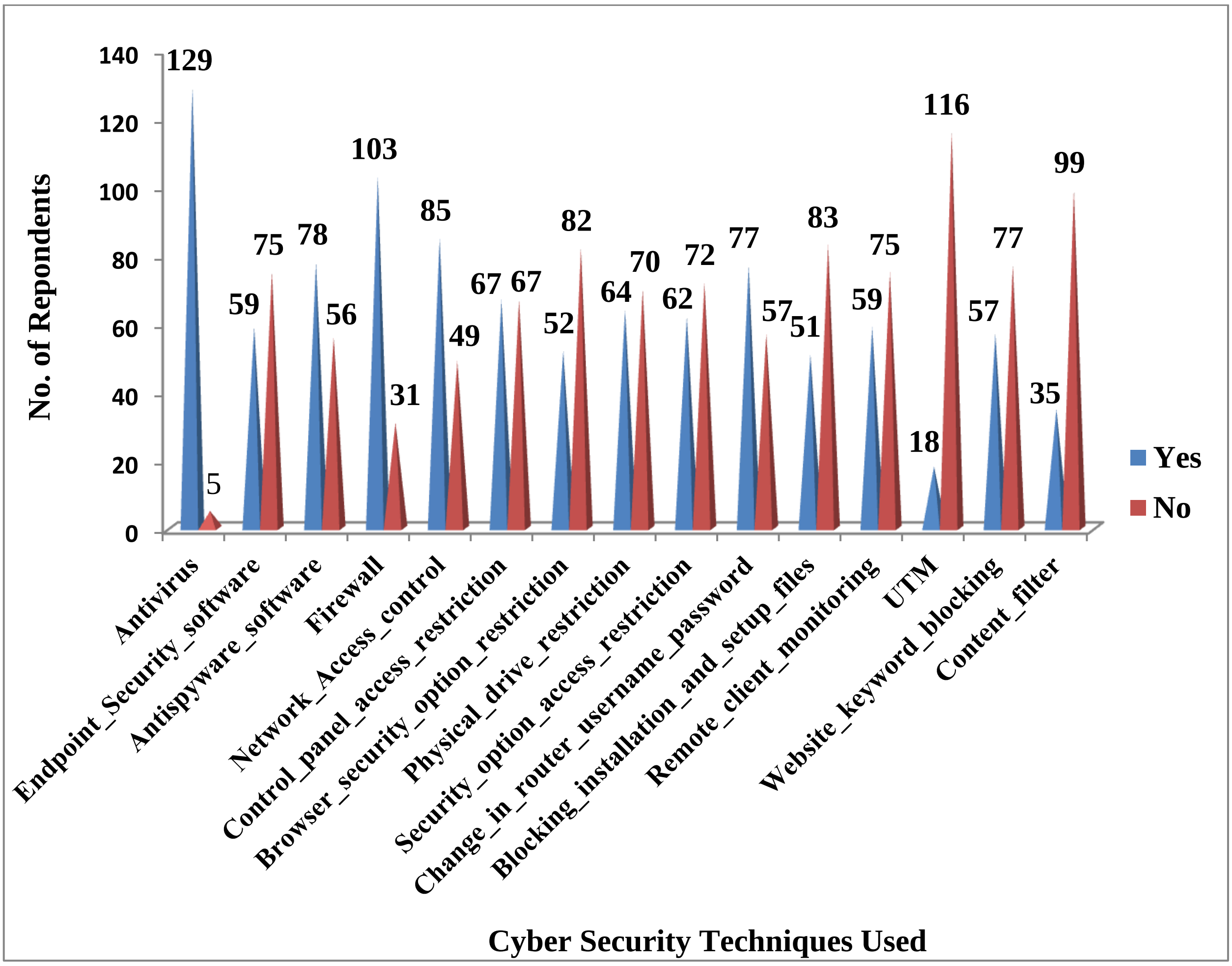
It is observed that 7.66 percent respondents are aware about Cyber security techniques to be used when making use of connection Type Wi-Fi to avoid Cyber-crimes which seems very less.

Table No. 5.10(A): Cyber Security Techniques used in Cyber Cafe

Sr. No.	Cyber Security Techniques Used	No. of Respondents		Total
		Yes	No	
1	Antivirus	129 (96.30)	5 (3.70)	134 (100)
2	End point security software	59 (44.50)	75 (55.50)	134 (100)
3	Antispyware software	78 (58.20)	56 (41.80)	134 (100)
4	Firewall	103 (76.90)	31 (23.10)	134 (100)
5	Network Access control	85 (63.40)	49 (36.60)	134 (100)
6	Control panel access restriction	67 (50)	67 (50)	134 (100)
7	Browser security option restriction	52 (38.80)	82 (61.20)	134 (100)
8	Physical drive restriction	64 (47.80)	70 (52.20)	134 (100)
9	Security option access restriction	62 (46.30)	72 (53.70)	134 (100)
10	Change in router username password	77 (57.50)	57 (42.50)	134 (100)
11	Blocking installation and setup files	51 (38.10)	83 (61.90)	134 (100)
12	Remote client monitoring	59 (44)	75 (56)	134 (100)
13	UTM	18 (13.40)	116 (86.60)	134 (100)
14	Website keyword blocking	57 (42.50)	77 (57.50)	134 (100)
15	Content filter	35 (26.10)	99 (73.90)	134 (100)
Total		996	1014	
Average Percentage		49.58	50.42	

Figures in bracket indicates Percentages

Graph 5.6(A): Cyber Security Techniques used in Cyber Cafe



From the Graph 5.6(A) it is clear that most of the respondents have Antivirus installed in the Cyber Cafe followed by Firewall security technique used. 63.40 percent respondents have network access security technique followed by Antispyware software with 58.20 percent respondents. Other securities techniques are also used such as Control panel access restriction, Browser Security option restriction, Blocking Installation and setup files and others.

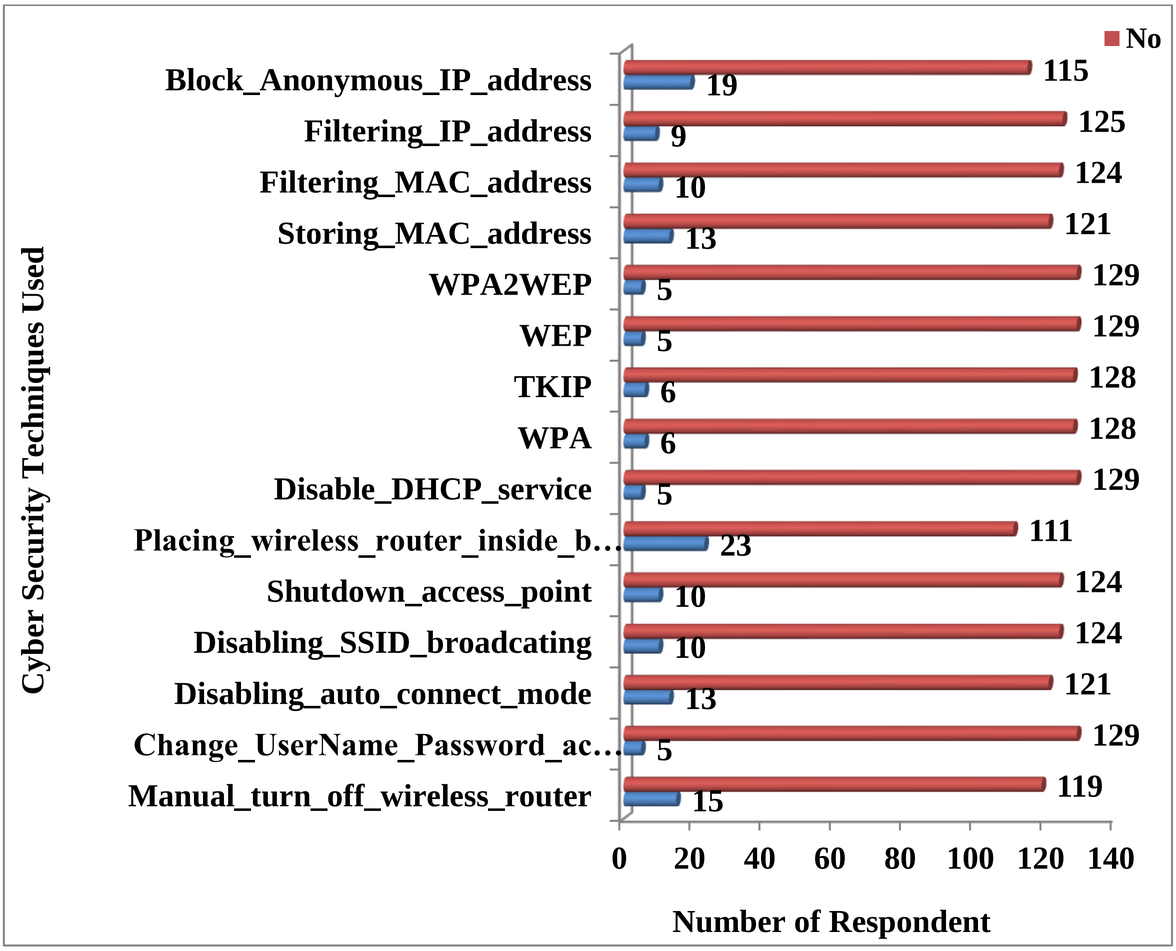
Table No. 5.10(B): Wi-Fi Cyber Security Techniques used in Cyber Cafe

Sr. No.	Cyber Security Techniques Used	No. of Respondents		Total
		Yes	No	
1	Manual turn off wireless router	15 (11.19)	119 (88.81)	134 (100)
2	Change User Name Password access point	5 (3.74)	129 (96.26)	134 (100)
3	Disabling auto connect mode	13 (9.71)	121 (90.29)	134 (100)
4	Disabling SSID broadcasting	10 (7.47)	124 (92.53)	134 (100)
5	Shutdown access Point	10 (7.47)	124 (92.53)	134 (100)
6	Placing wireless router inside building	23 (17.17)	111 (82.83)	134 (100)
7	Disable DHCP service	5 (3.74)	129 (96.26)	134 (100)
8	WPA	6 (4.47)	128 (95.53)	134 (100)
9	TKIP	6 (4.47)	128 (95.53)	134 (100)
10	WEP	5 (3.74)	129 (96.26)	134 (100)
11	WPA 2	5 (3.74)	129 (96.26)	134 (100)
12	Storing MAC Address	13 (9.71)	121 (90.29)	134 (100)
13	Filtering MAC Address	10 (7.47)	124 (92.53)	134 (100)
14	Filtering IP Address	9 (6.72)	125 (93.28)	134 (100)
15	Block Anonymous IP Address	19 (14.18)	115 (85.82)	134 (100)
Total		154	1856	
Average Percentage		7.66	92.34	

Figures in bracket indicates Percentages

Table No.5.10 (B) shows that 11.90 percent respondents Turn off Wireless Router manually, 3.74 percent respondents change Username and Password of access point, 9.71 percent respondents disable auto connect mode, 7.47 percent respondents shutdown access point, 17.70 percent respondents place wireless router inside building, 3.74 percent respondents disable DHCP service, 4.47 percent respondents make use of WPA protocol, 4.47 percent respondents make use of TKIP protocol, 3.74 percent make use of WEP and WPA2 protocol, 9.71 percent respondent store MAC address, 7.47 percent respondents use filter MAC address and14.18 percent block anonymous IP address.

Graph 5.6(B): Wi-Fi Cyber Security Techniques used in Cyber Cafe



From the Graph 5.6 (B), it is clear that respondents are not using security Techniques when making use of Wi-Fi. Very less percentage of respondents use wireless security techniques for the Cyber Cafe such as placing the router inside the building, Block anonymous IP address, Manual Turn off wireless router, storing MAC address and disabling auto connect mode which has more percentage as compared to other parameters.

5.5.3 Physical Cyber Security Techniques used in Cyber Cafe

As Cyber security is important to prevent Cyber-crimes and unlawful act so along with technical Cyber security physical Cyber security is also required. Table No. 5.11 shows that 20.90 percent respondents lock opening windows followed by 7.50 percent respondents using locking of PC cases, 2.20 percent respondents use break alarm sensors, 6.70 percent respondents use intruders alarms sensor on access router so that unknown intruders can be identified immediately, 8.20 percent respondents have separate server installed whereas no one uses detectors in Cyber Cafe to check for unlawful act.

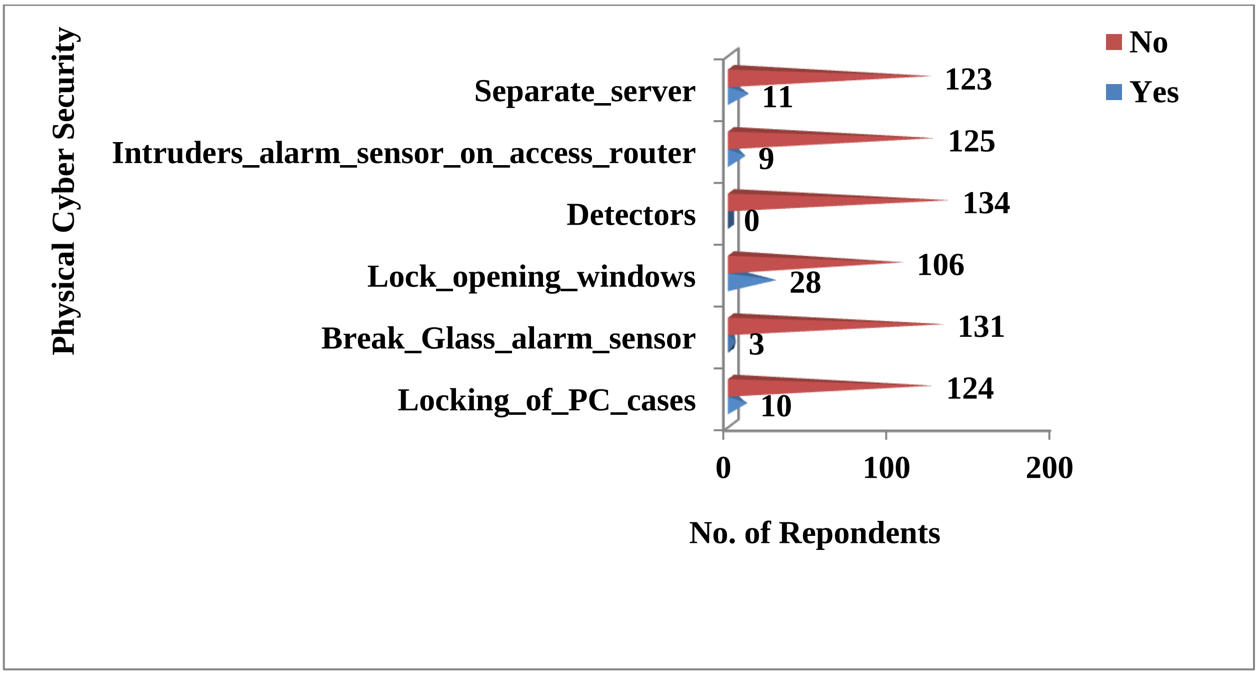
As seen from the table, 92.42 percent respondents are not implementing physical security in Cyber Cafe which is very important so that evidences are not lost in case a crime takes place.

Table No. 5.11: Physical Security Techniques used in Cyber Cafe

Sr. No.	Physical Cyber Security	No. of Respondents		Total
		Yes	No	
1	Locking of PC Cases	10 (7.50)	24 (92.50)	134 (100)
2	Break Glass alarm sensor	0.3 (2.20)	131 (97.80)	134 (100)
3	Lock Opening Windows	28 (20.90)	106 (79.10)	134 (100)
4	Detectors	0 (0)	134 (100)	134 (100)
5	Intruders Alarm Sensor on Access Router	0.9 (6.70)	125 (93.30)	134 (100)
6	Separate Server	11 (8.20)	123 (91.80)	134 (100)
Total		50.20	743	
Average Percentage		7.58	92.42	

Figures in bracket indicates Percentages

Graph 5.7: Physical Cyber Security Techniques implemented in Cyber Cafe



From Graph 5.7, it clears that only 20.90 percent of respondents use physical security technique that is locking windows so that theft cannot take place. Other techniques such as locking of PC cases or using alarm sensors on routers and break glass alarms or detectors. Very few respondents have separate server room for servers. This shows that respondents are not aware about physical Cyber security and presently have not implemented it in Cyber Cafe.

5.5.4 Summary

Majority of Owners maintain Cyber security at Gateway level and make use of self method for implementation. This shows that they are aware about maintaining Cyber security in Cyber Cafe. Various techniques are used to implement Cyber security such as installing of security software's like antivirus, antispyware and firewall. Apart from these techniques, they used Network access control, Control panel access restrictions and use of the device such as UTM. Physical Cyber security such as locking of PC cases, Break glass alarm sensor, locking of open windows, Detectors and alarm sensors etc. Physical security is maintained by less number of Owners which should be improved. Overall it is observed that Owners are aware about technical Cyber security and are implementing it at their Cyber Cafe but need to improve physical Cyber security. They are aware about Broadband connection security techniques and at a good extent try to implement them but when using Broadband Wi-Fi, most of the Owners are not making use of Cyber security techniques. Wi-Fi is growing at a greater extent and is considered most unsecured so security techniques need to be implemented at a large extent by Owners.

5.6 Rules and Regulation of Cyber Security and their Impact on Cyber Cafe Owners

Governments of India have enforced rules and regulation for Cyber Cafe in India. Cyber Café Owners should follow these rules. Identification of User by establishing his or her identity with a document, maintaining log registers, maintaining records such as history of websites accessed, proxy server logs, mail server logs, logs of network device and firewall and intrusion prevention or detection system used. Also Owners should follow infrastructure guidelines provided by government related to size and height of cubicles, Installation of illegal or banned software such as deep freeze should be not allowed. Various display board such as prohibiting Visitors from viewing pornographic sites should be displayed in Cyber Cafes. Owners should refer to "Guidelines for auditing and logging – CISG-2008-01" prepared by Indian Computer Emergency Response Team (CERT-In) for any assistance related to logs. Minors should not be allowed to use Cyber café internet services unless accompanied by an elderly person.

Due to the imposition of rules and regulations the Cyber Cafe businesses have been adversely affected. Many of the Cyber Cafes are on the verge of closing down. A Cyber Cafe Owners feels that there is a huge decline in numbers of Visitors but on the other side people are getting more aware about Cyber-crime. An attempt was made to meet the objective of the study which is "*To observe the impact of Cyber security rules and regulations on Cyber Cafe Owners and Visitors*." Such an analysis aims to know the impact of Cyber security rules and regulation on Cyber Cafe Owners in Pune City.

An attempt has been made to study the impact of Cyber security rules and regulations on Owners by noting some observations.

5.6.1 Provision of Cyber-crime prevention in Cyber Cafe

For Cyber-crime prevention all Cyber Cafe Owners make provision in the café such as displaying posters of restricted websites and government rules. Table No.5.12

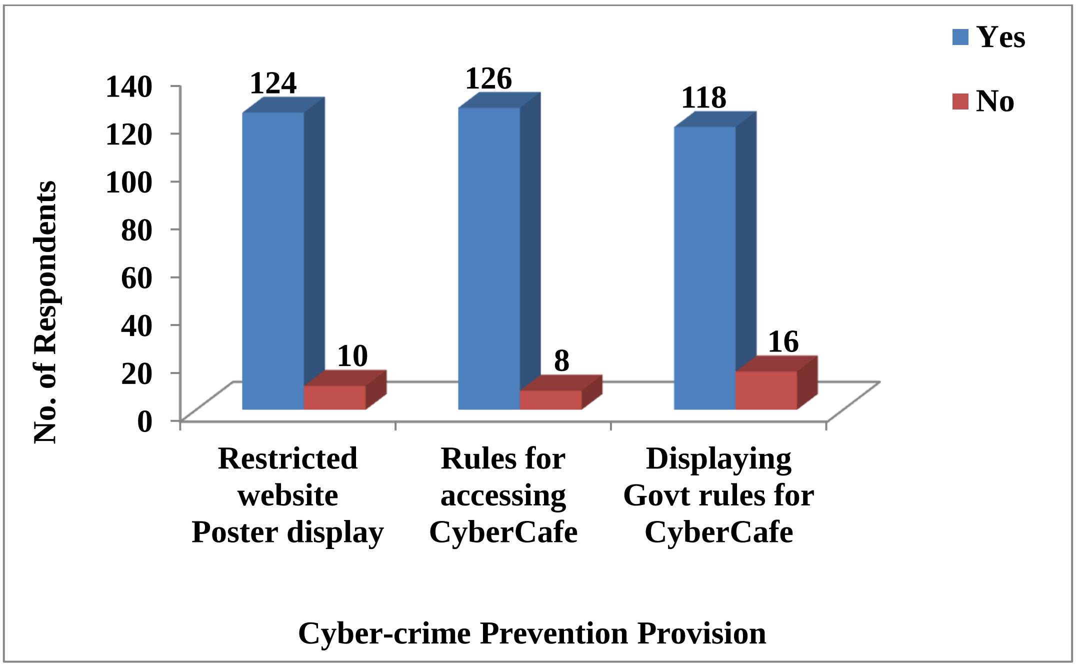
shows the distribution of the respondents according to their implementation of existing Cyber Cafe security rules and regulation provided by the government. It is seen that 92.50 percent of respondent display poster of website which are restricted such as pornographic websites. 94 percent of respondent display rules for accessing cyber cafe such as login details and 88.10 percent respondents display government rules and regulations for cyber cafe. It is seen that 91.53 percent respondents on an average take steps for Cyber-crime prevention provision. This is good step towards Cyber-crime prevention.

Table No.5.12: Cyber-crime Prevention Provision

Cyber-crime Prevention provision	**No. of Respondents**		**Total**
	Yes	**No**	
Restricted website Poster display	124 (92.50)	10 (7.50)	134 (100)
Rules for accessing Cyber Cafe	126 (94.0)	8 (6.0)	134 (100)
Displaying Government rules for Cyber Cafe	118 (88.10)	16 (11.90)	134 (100)
Total	368	34	
Average Percentage	91.53	8.46	

Figures in bracket indicates Percentages

Graph 5.8: Cyber-crime Prevention Provision



The Graph 5.8 clearly indicates that 91.53 percent respondents are aware and follow the Cyber-crime prevention provision by the government, 92.50 percent respondents display poster for restricted website and 88.10 percent respondents display government rules for Cyber Cafe. Hence it is clear that Cyber Cafe respondents follow Cyber-crime prevention measures imposed by the government.

5.6.2 Log Register for Activities and Various Physical Resources used in Cyber Cafe.

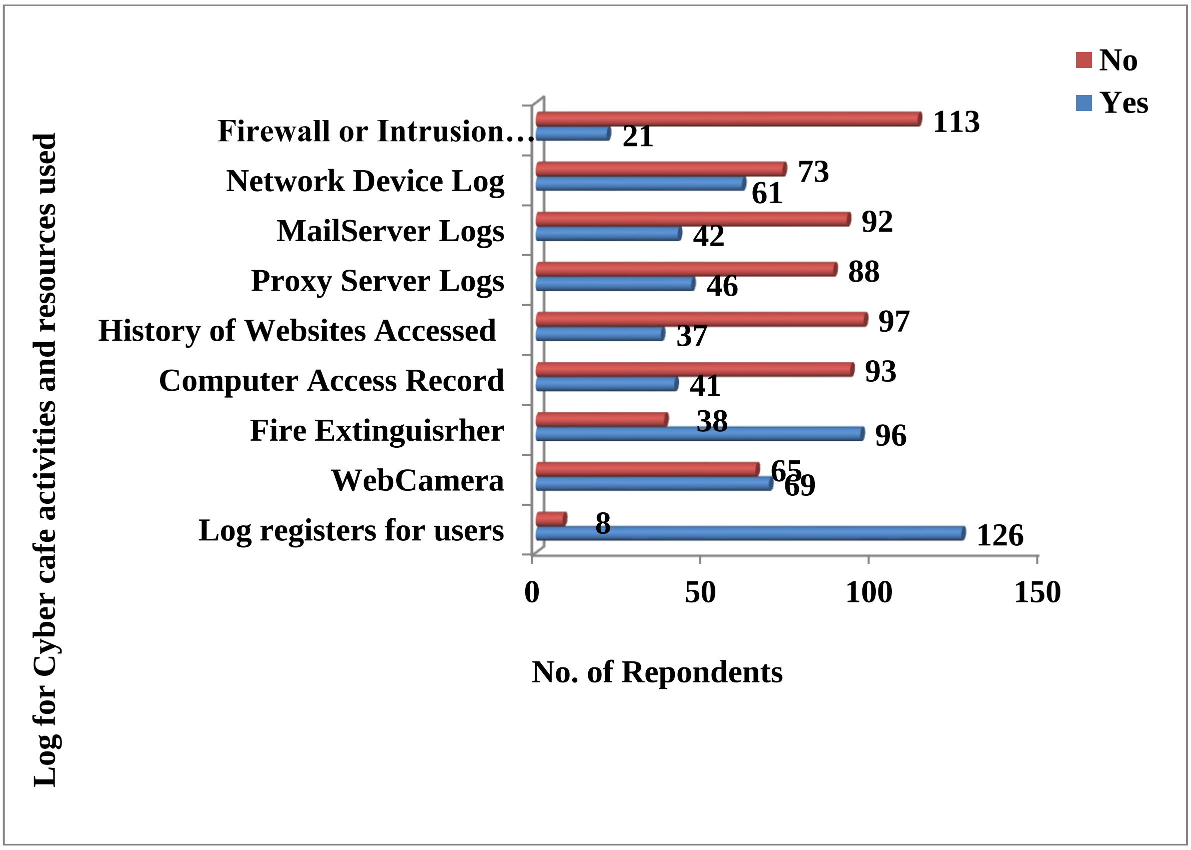
In a Cyber Cafe many physical resource logs are to be maintained as per government rules and regulations. Table No.5.13 shows that 94 percent of respondents maintain users log register that consist of their identification proof and other details.51.50 percent respondents have web camera installed.71.60 percent respondents have fire extinguisher for safety. 30.60 percent respondents maintain computer access record along with 27.60 percent respondents maintain History of websites accessed using computer resource at Cyber Cafe, 34.30 percent respondents maintain Logs of proxy server installed at Cyber Cafe, 31.30 percent respondents maintain Mail server logs, 45.50 percent respondents maintain Logs of network devices such as router, switches, systems etc. installed at Cyber Cafe and 15.70 percent respondents maintain Logs of firewall or Intrusion Prevention/Detection systems, if installed. On an average 44.68 percent respondents maintain logs for Cyber Cafe activities and resources used. These needs to be improved since log registers are important resources to track Cyber-crime in case it occurs.

Table No.5.13: Log for Cyber Cafe activities and resources used

Log for Cyber Cafe activities and resources used	**No. of Respondents**		**Total**
	Yes	**No**	
Log registers for users	126 (94.0)	8 (6.0)	134 (100)
Web Camera	69 (51.50)	65 (48.50)	134 (100)
Fire Extinguishers	96 (71.60)	38 (28.40)	134 (100)
Computer Access Record	41 (30.6)	93 (69.40)	134 (100)
History of Websites Accessed	37 (27.60)	97 (72.40)	134 (100)
Proxy Server Logs	46 (34.30)	88 (65.70)	134 (100)
Mail Server Logs	42 (31.30)	92 (68.70)	134 (100)
Network Device Log	61 (45.50)	73 (54.50)	134 (100)
Firewall or Intrusion Prevention/Detection Log	21 (15.70)	113 (84.30)	134 (100)
Total	539	667	
Total Average	44.68	55.32	

Figures in bracket indicates Percentages

Graph 5.9: Log for Cyber Cafe Activities and Resources used



The Graph 5.9 clearly indicates that 94 percent respondents maintain log registers of Visitors which are most important as per the government rules and regulations. Other logs such as computer access record, proxy server log, mail server log, network device log, Firewall or intrusion prevention or detection log are maintained but by less respondents. 51.50 percent respondents maintain web camera details and 71.60 percent respondents have fire extinguisher. It is clear that respondents are aware about rules and regulations and follow them in their Cyber Cafe but still only 44.68 percent respondents maintain the log which should be increased.

5.6.3 Visitors Identification Documents.

As per government rules it is mandatory to verify Visitors identification by checking documents that Visitors establish such as identity card issued by any School or

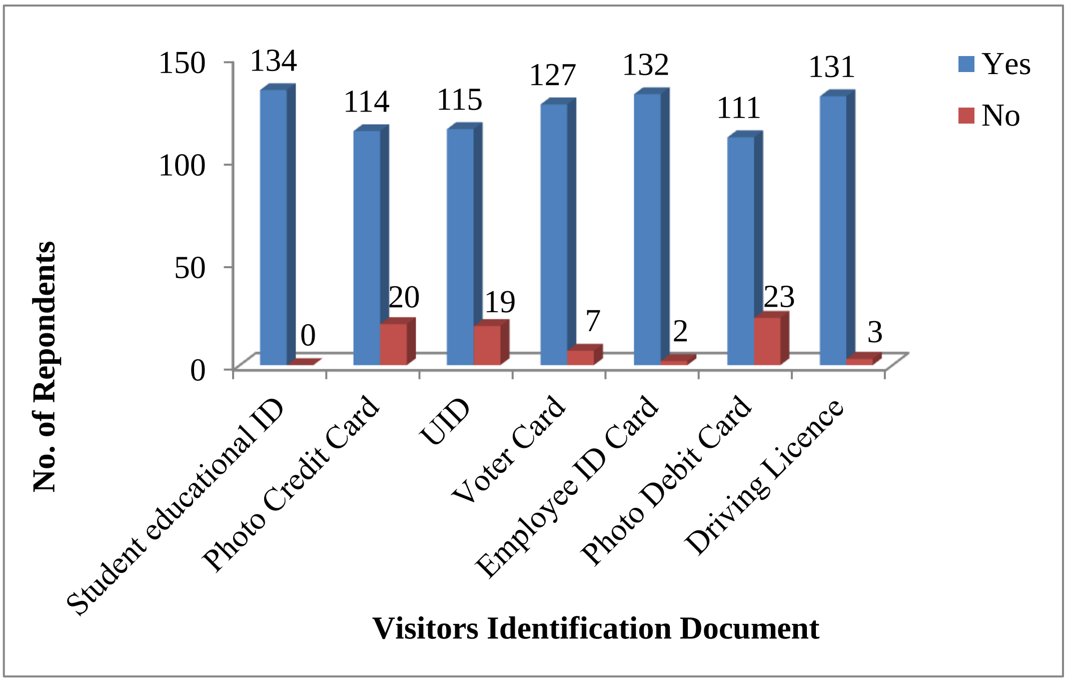
College, Photo Credit Card or debit card issued by a Bank or Post Office, Passport, Voters Identity Card, Permanent Account Number (PAN) card issued by Income-Tax Authority, Photo Identity Card issued by the employer or any government agency, Driving License issued by the appropriate government. From the Table No. 5.14 it is seen that all respondents agreed that for verification purpose they allow student educational ID as ID proof, 85.10 percent respondents allow photo Credit Card, 85.80 percent respondents allow UID card as ID proof, 94.8 percent respondents allow Voter ID card followed by 98.50 percent respondents allowing employee ID, 82.80 percent respondents allowing photo Debit card and 97.80 percent respondents allowing Driving License as ID proof. It is seen on an average 92.11 percent of respondents check identification documents of Visitors. Each Cyber Café Owners use standard Identity checking policy. In future it can be used to trace Cyber criminal.

Table No.5.14 Visitors Identification Document

Visitors Identification	No. of Respondents		Total
	Yes	No	
Student educational ID	134 (100.0)	0 (0.0)	134 (100)
Photo Credit Card	114 (85.10)	20 (14.90)	134 (100)
UID	115 (85.80)	19 (14.20)	134 (100)
Voter Card	127 (94.80)	7 (5.20)	134 (100)
Employee ID Card	132 (98.50)	2 (1.50)	134 (100)
Photo Debit Card	111 (82.80)	23 (17.20)	134 (100)
Driving License	131 (97.80)	3 (2.20)	134 (100)
Total	864	74	
Average Percentage	92.11	7.89	

Figures in bracket indicates Percentages

Graph 5.10: Visitor Identification Document



Form the Graph 5.10 it is clear that Cyber Cafe Owners verify Visitors Identification by checking their Identification documents that they provide. All respondents allow Visitors to use Cyber Cafe services by verifying student educational ID, followed by 94.80 percent respondents allow Voter ID card followed by 98.50 percent respondents allowing employee ID along with other proof such as UID, Photo debit or Credit card or Driving License. Thus it is apparent that respondents follow Cyber Cafe rules and regulation by checking the ID proof of Visitors.

5.6.4 Physical Layout and Computer Resource in Cyber Cafe

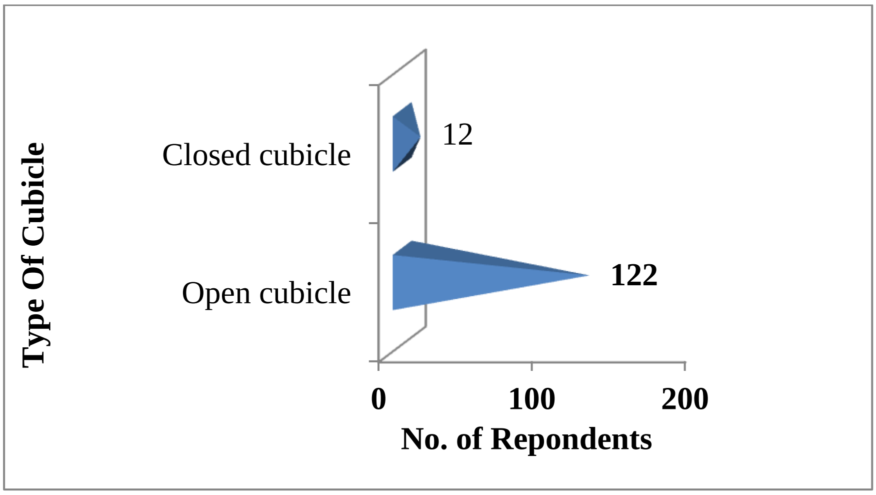
Partitions of Cubicles built or installed if any, inside the Cyber Cafe, should be open and not closed cubicles. The screen of all computers, installed other than in partitions or Cubicles, shall face ‘outward’, i.e. they shall face the common open space of the Cyber Cafe. From the Table No.5.15 it is seen that 91 percent Cyber cafe have open cubicles where as only 9 percent Cyber Cafe still have closed cubicles.

Table No.5.15: Types of Cubicle in Cyber Cafe.

Sr. No	Types of Cubicles	No Of Respondent
1	Open Cubicle	122 (91.0)
2	Closed Cubicle	12 (9.0)
Total		134 (100)

Figures in bracket indicates Percentages

Graph 5.11: Type of Cubicle



From the Graph 5.11 it is clear that most of the Cyber cafes that are 91 percent have open cubicles and very less number of Cyber cafes still has closed cubicles. Thus it is clear that respondents are aware and follow the rules and regulations laid by the government.

5.6.5 Cubicle Partition Height

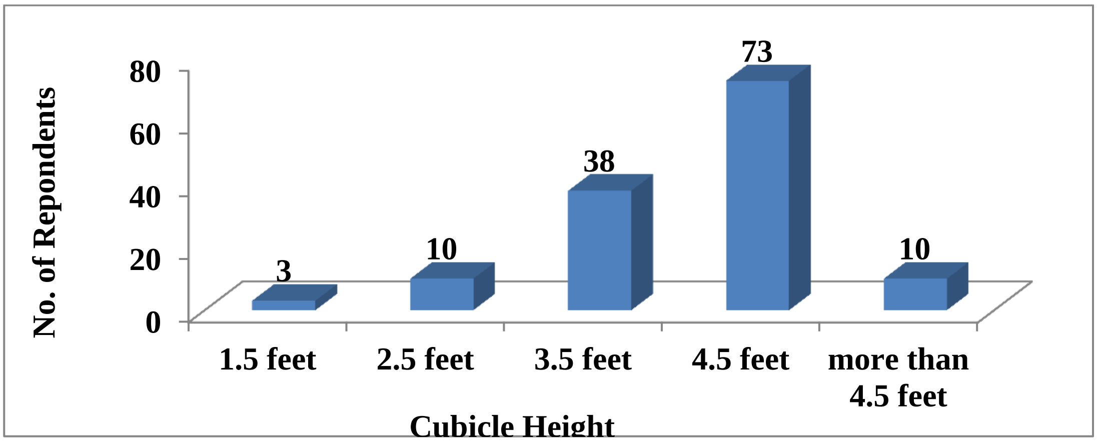
Partitions of Cubicles built or installed if any, inside the Cyber Cafe, should be open and not closed cubicles and should not exceed four and half feet in height from the floor level as per government rules and regulations. From the Table No.5.16 it is clear that 54.50 percent Cyber cafe have cubicles or partition height as 4.5 feet and 28.30 percent Cyber cafe have 3.5 feet height followed by 7.50 percent Cyber cafe with 2.5 feet height and 2.20 percent Cyber cafe have 1.5 feet of cubicle height. Only 7.50 percent Cyber cafe have cubicle height more than 4.5 feet which means they are not aware about the rules and regulation of Cyber Cafe.

Table No.5.16: Cubicle Height in Cyber Cafe.

Sr. No	Cubicle Height	No Of Respondent
1	1.5 feet	3 (2.20)
2	2.5 feet	10 (7.50)
3	3.5 feet	38 (28.30)
4	4.5 feet	73 (54.50)
5	More than 4.5 feet	10 (7.50)
Total		134 (100)

Figures in bracket indicates Percentages

Graph 5.12: Cubicle Height



From the Graph 5.12 it is clear that most of the respondents are aware about Cyber Cafe rules and regulation since most of the respondents that is 54.50 percent have cubicle or partition height 4.5 feet. Thus it shows that respondents are aware about Cyber Cafe rules and regulations regarding size of cubicles.

5.6.6 Infrastructure & Technical Details

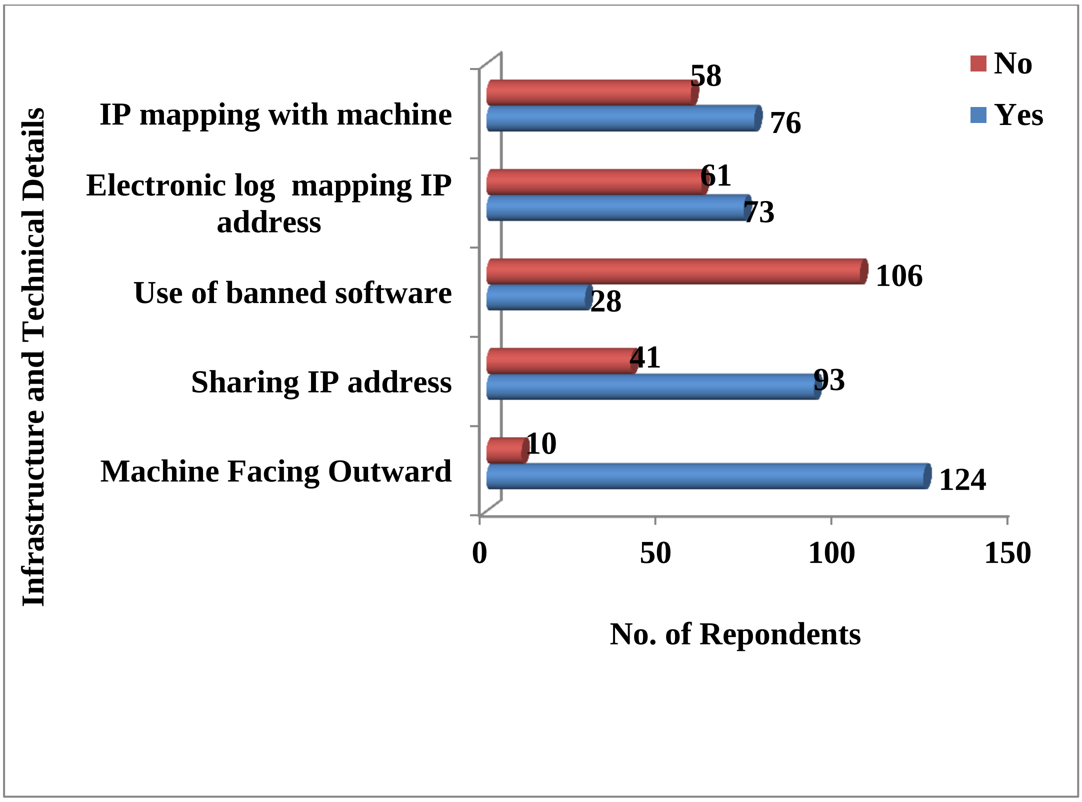
According to government there are infrastructure and Technical details that have to be followed by Cyber Cafe Owners. Banned software such as Deepfreeze should not be used in Cyber Cafe which deletes all log details. Machines should be facing outward .Table No. 5.17 shows that 92.50 percent respondents have computer machines in Cyber Cafe facing outward. 69.40 percent respondents have shared IP address and 56.70 percent respondents have IP mapping with machine. 54.50 percent respondents keep electronic log of mapping with masqueraded IP address and 20.90 respondents still use banned software such as Deepfreeze. It is seen that on an average 58.80 percent respondent follow infrastructure and technical rules as per the government rules. 41.20 percent respondents still do not follow infrastructure and technical rules.

Table No.5.17: Infrastructure &Technical Details

Infrastructure & Technical Details	Yes	No	Total
Machine Facing Outward	124 (92.50)	10 (7.50)	134 (100)
Sharing IP address	93 (69.40)	41 (30.60)	134 (100)
Use of banned software	28 (20.90)	106 (79.10)	134 (100)
Electronic log of mapping with masqueraded IP address	73 (54.50)	61 (45.50)	134 (100)
IP mapping with machine	76 (56.70)	58 (43.30)	134 (100)
Total	394	276	
Average Percentage	58.80	41.20	

Figures in bracket indicates Percentages

Graph 5.13: Infrastructure and Technical Details



Form the Graph 5.13 it is observed that 92.5 percent respondents have computer machines in Cyber Cafe facing outward. 69.40 percent respondents have shared IP address and 56.70 percent respondents have IP mapping with machine. 54.50 percent respondent keep electronic log of mapping with masqueraded IP address and 20.90 respondents still use banned software such as Deepfreeze because they are not aware about it and 79.10 percent respondents do not use it. Thus respondents are aware that machines should be facing outwards, if IP is shared then electronic log of IP mapping with machine should be kept, Banned Software such as Deepfreeze should not be used.

5.6.7 Cyber Café Owners view about Cyber Cafe rules and Regulation

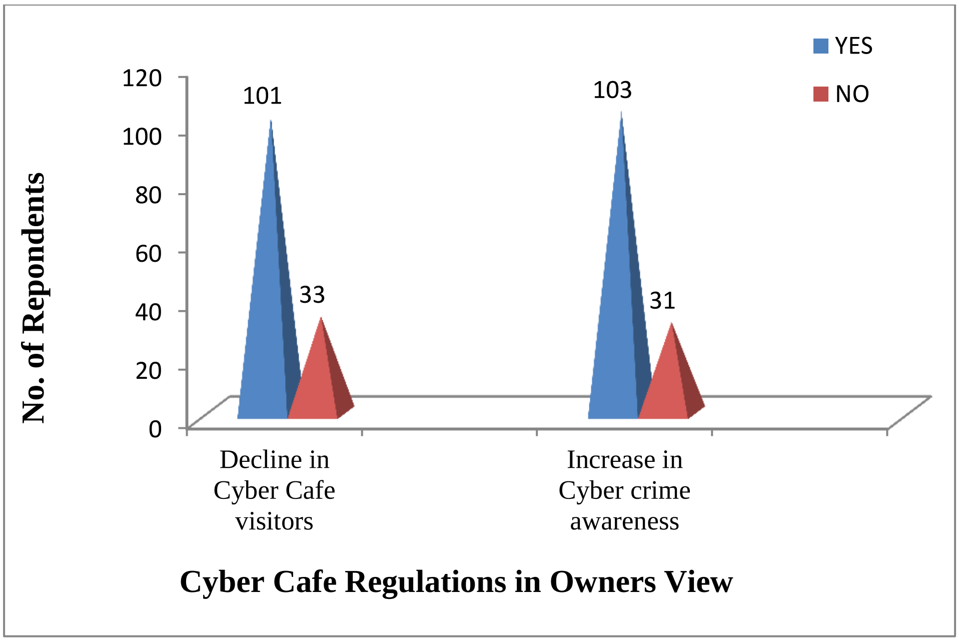
Due to the Rules and regulations imposed by the government the Owners are not happy and feel that it affects their business. From Table No.5.18 it is seen that 75.37 percent respondents feel that due to the rules and regulations imposed by the government there is a decline in number of Visitors in Cyber Cafe.76.38 percent respondents feels that there is increase in Cyber-crime awareness among Visitors.

Table No.5.18: Cyber Cafe Owners view about Cyber Cafe rules and Regulation

Cyber Cafe regulation in Owners view	No of respondent		Total
	YES	NO	
Decline in Cyber Cafe Visitors	101 (75.37)	33 (24.63)	134 (100)
Increase in Cyber-crime awareness	103 (76.86)	31 (23.14)	134 (100)

Figures in bracket indicates Percentages

Graph 5.14: Cyber Cafe Owners view about Cyber Cafe rules and Regulation



Form the Graph 5.14 it clears that 75.37 percent of the Cyber cafes respondents strongly feel that due to government rules and regulations there is decline in cyber cafe Visitor and their business is hampered. Also most of the respondents agreed that there is increase in cybercrime awareness due to government rules and regulations.

5.6.8 Audit For Cyber Cafe

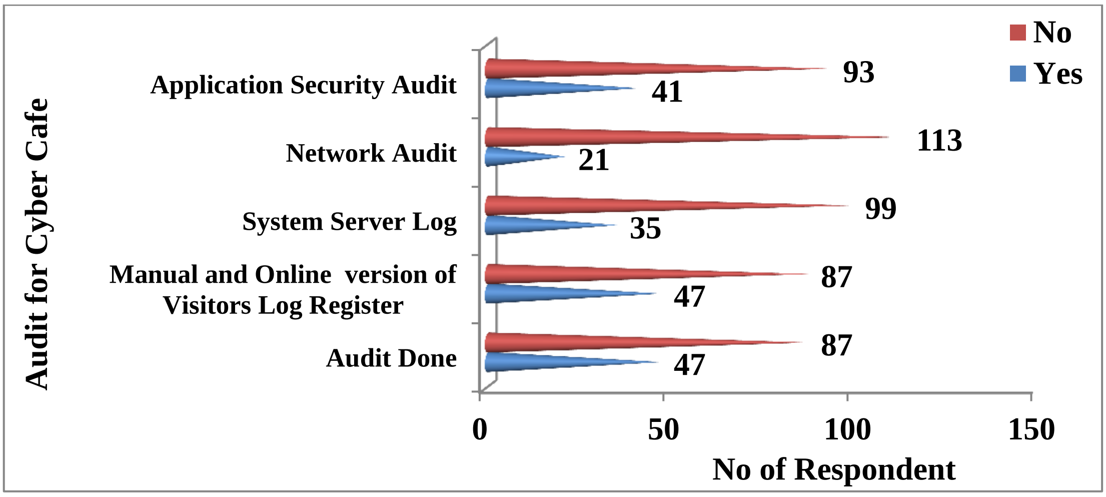
As per law every Cyber Cafe has to do audit by Government official whose rank is not below the rank of Police Inspector as authorized by the licensing agency. The government official check or inspect Cyber Cafe and the computer resource or network established at any time for the compliance of these rules. Different log sources needs to be checked such as Application log(web server, mail server, database server),System Sever log, Manual and online version of Visitors log and Network log (firewall log, IDS log/IPS log). Table No.5.19 shows 35.07 percent respondents agree that Audit is done for Cyber Cafe whereas 64.92 percent respondents do not agree to this. 35.07 percent respondents responded that Manual and Online version of Visitors Log Register Audit is done for Cyber Cafe. 26.12 percent respondents responded that System server log are checked, 15.67 percent respondents agreed that Network audit is done and 30.59 percent respondents responded that Application Security Audit is done. Thus it clearly signifies that only 28.51 percent respondents agree that audit for various log sources are done as per government guidelines on an average which is very less percentage.

Table No.5.19: Audit for Cyber Cafe

Sr. No	Audit For Cyber Cafe	No. of Respondents		Total
		Yes	No	
1	Audit Done	47 (35.07)	87 (64.92)	134 (100)
2	Manual and Online version of Visitors Log Register	47 (35.07)	87 (64.92)	134 (100)
3	System Server Log	35 (26.12)	99 (73.88)	134 (100)
4	Network Audit	21 (15.67)	113 (84.32)	134 (100)
5	Application Security Audit	41 (30.59)	93 (69.41)	134 (100)
Total		191	479	
Average Percentage		28.51	71.49	

Figures in bracket indicates Percentages

Graph 5.15: Audit for Cyber Cafe



From the Graph No.5.15 it is clear that in most of the cyber cafe the Audit is not done since 64.92 percent respondents agreed to this. As per government rule for cyber café, Manual and Online version of Visitors Log Register, System Server Log, Network Audit, Application Security audit should be done. From the graph it is clear that it audit is done at less than 30 percent cyber cafe.

5.6.9 Summary

Government has laid Rules and Regulation for Cyber Cafe. It is observed that Owners follow the Rules and Regulation. Most of the Owners display posters for restricted website, along with displaying Rules and Regulations that should be followed by Visitors. Most of the Owners maintain log registers for various activities of Visitors. Many Owners maintain web camera and store its details. Details about computer access record, History of websites access and, mail server log are maintained by less number of Owners. Firewall or Intrusion Prevention /Detection Log is also maintained by very few Owners. It is observed that Owners do the Visitors Identification of document which is mandatory and also maintain a record of it. Cubicles in Cyber Cafe are mostly open cubicles, closed cubicles are not allowed in Cyber Cafe. Height of the cubicle partition is found to be less than or equal to 4.5 feet. Very few Owners use Banned Software such as Deep Freeze. Details regarding Electronic log of mapping with masqueraded IP address is maintained by many Owners. It is observed that Owners feel that due to the Rules and Regulations there is decline in Cyber Cafe Visitors but there is increase in Cyber-crime awareness among Visitors. Most of the Owners agreed that audit of cyber cafe is not done by government officials as per rules and regulations.

5.7 Presentation and Analysis of Data II: Cyber Cafe Visitors

The Visitor’s analysis is carried out in three broad headings and is as follows:

1. General background of the Visitors with respect to their gender, age and Cyber Cafe usage.
2. Awareness of Cyber Cafe Visitors regarding Cyber security management and Cyber-crime.
3. Impact on cyber cafe Visitors of Cyber security rules and regulations on the usage of Cyber Cafe services.

Introduction

In this section the researcher has analyzed the primary data collected from 384 Visitors from Cyber Cafes in Pune city. Visitors visit Cyber Cafe for various activities such as social networking, shopping, E-governance service, Net Banking etc. They pay fees per hour for using the internet service. They are benefited by Cyber Cafe for many probable reasons such as they can get assistance in case they are finding it difficult to use the internet, they can use latest software available, also the speed of internet that they get is good. They follow the rules and regulations for the Cyber Cafe. Most of the Visitors are aware about various types of crimes and Cyber security rules and regulations.

The objective of the study is *“To study the awareness of Cyber security management among Owners and Visitors of Cyber Cafe and to study the present cyber security provided in cyber cafes by Owners.”* To study this objective, the researcher has collected data from 384 Visitors from various Cyber Cafes who visit Cyber Cafe for internet services.

5.8 General Background of the Visitors according to their Age and Gender

Table No.5.20 shows the distribution of respondents according to their age and gender. It is seen that most of the respondents who come to Cyber Cafe are Male with 57.82 percent and 42.18 percent are Female. Respondents in between age group

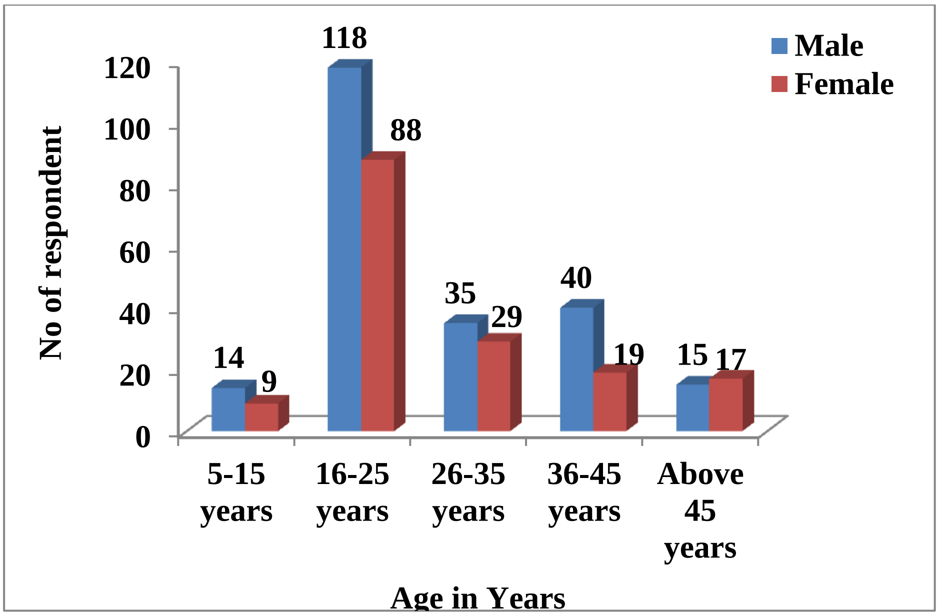
5 to 15years are 5.98 percent out of which 3.64 percent respondents are male and 2.34 percent respondents are female. Between age group 16 to 25 years total respondents are 53.63 percent respondents which is maximum out of which 30.72 percent respondents are male and 22.91 percent respondents are female. Between age group 26 to 35 years the total respondents are 16.66 percent out of which 9.11 percent respondents are male and 7.55 percent respondents are female. Between age group 36 to 45 years total respondents are 15.35 percent out of which 10.41 percent respondents are male and 4.94 percent are female. Above 45 years of age total respondents are 8.38 percent out of which 3.96 percent respondents are male and 4.42 percent respondents are female. Thus it is clear that most of the respondents belong to the age group 16 to 25 years who come for internet service access. Also on an average 57.82 percent respondents belong to Male category and 42.18 percent belong to Female category.

Table No.5.20: Distribution of Visitors according to their Age and Gender

Sr. No	**Age in Years**	**Gender**		**Total**
		Male	**Female**	
1	5-15 years	14 (3.64)	9 (2.34)	23 (5.98)
2	16-25 years	118 (30.72)	88 (22.91)	206 (53.63)
3	26-35 years	35 (9.11)	29 (7.55)	64 (16.66)
4	36-45 years	40 (10.41)	19 (4.94)	59 (15.35)
5	Above 45 years	15 (3.96)	17 (4.42)	32 (8.38)
Total		222 (57.82)	162 (42.18)	384 (100)

Figures in bracket indicates Percentages

Graph 5.16: Distribution of Visitors according to their Age and Gender



The Graph 5.16 shows the distribution of respondents according to their age and gender. It is clearly seen that most of the respondents who come to Cyber Cafe are between the age group 16 to 25 years. Ratio of female respondents is slightly less than the Male Visitors.

5.8.1 Visitors visit to Cyber Cafe

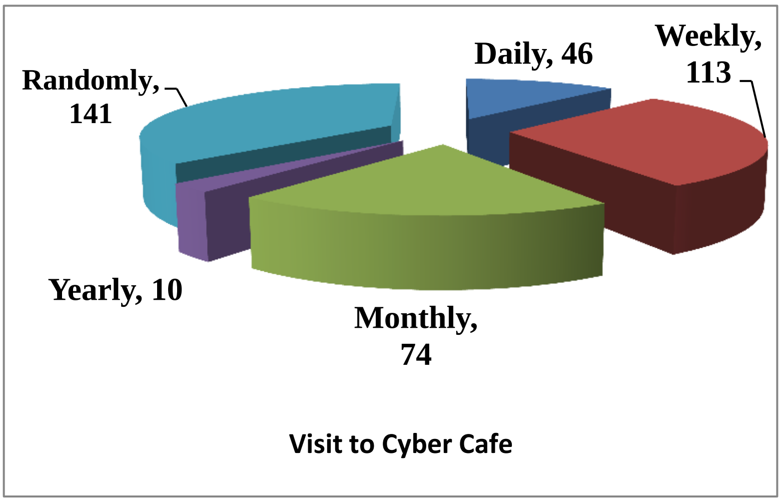
The Table No.5.21 shows that 12.0 percent respondents visit Cyber Cafe on daily basis whereas 29.40 percent respondents visit Cyber Cafe weekly. Further 19.30 percent respondents visit Cyber Cafe monthly followed by 2.60 percent respondents visiting Cyber Cafe yearly and 36.70 percent respondents visiting Cyber Cafe randomly. It is very clear that maximum Visitors visit Cyber Cafe weekly for accessing internet services.

Table No.5.21: Cyber Cafe visit Frequency

Sr. No	Visit to Cyber Cafe	No of Respondent
1	Daily	46 (12.0)
2	Weekly	113 (29.40)
3	Monthly	74 (19.30)
4	Yearly	10 (2.60)
5	Randomly	141 (36.70)
Total		384(100)

Figures in bracket indicates Percentages

Graph 5.17: Cyber Cafe visit Frequency



The Graph 5.17 clearly states that most of the respondents visit Cyber Cafe randomly or weekly followed by few respondents visit Cyber Cafe monthly followed by daily whereas ratio to visit cyber cafe yearly is very low as compared to others.

5.8.2 Probable Reasons for Visiting the Cyber Cafe

Visitors use Cyber Cafe for many reasons. Internet Service provided by Cyber Cafe has many advantages as compared to home users or mobile internet. Table No. 5.22

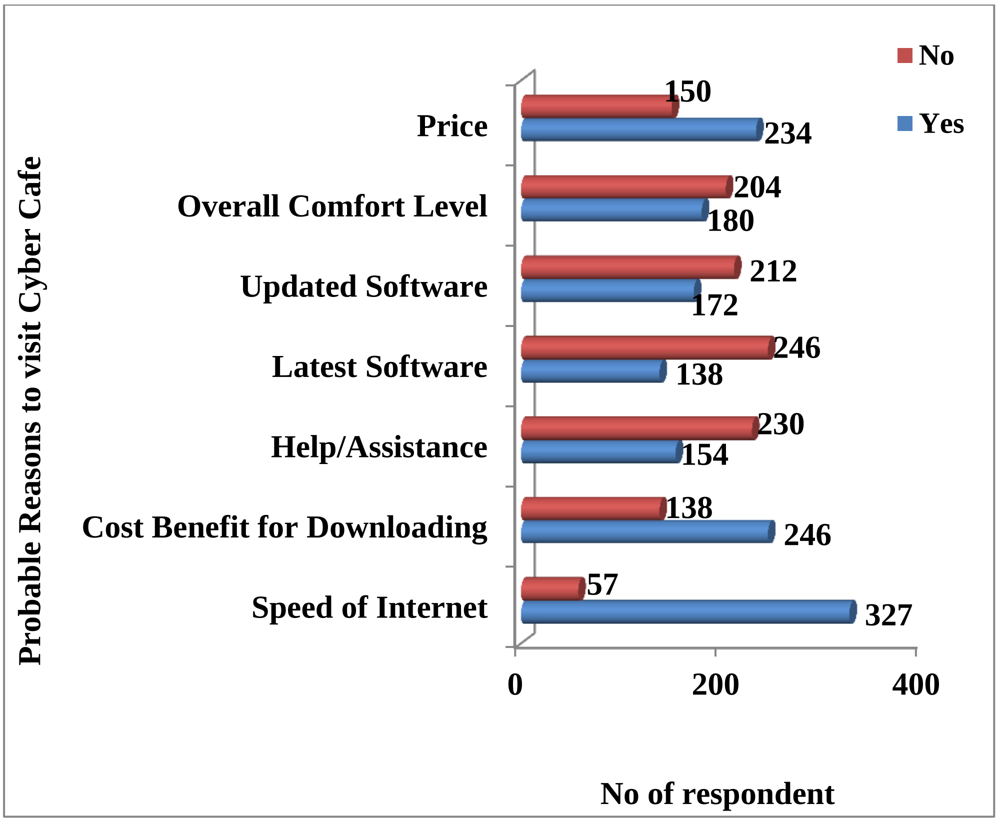
shows 85.20 percent respondents visit Cyber Cafe for speed of internet, 64.10 percent respondents use cafe for cost benefit for downloading, 40.1 percent respondents uses for Help or assistance, 35.90 percent respondents uses cafe because they can get latest software to use, 44.80 percent respondents visit Cyber Cafe because they can get updated software to use. 46.90 percent respondents use Cyber Cafe because they find it more comfortable followed by 60.90 percent respondents who feel that the price they have to pay is less and affordable. On an average 53.98 percent respondents find Cyber Cafe option ad good, compared to other internet services that are available.

Table No.5.22: Reasons to Visiting Cyber Cafe Visitors

Sr. No	Probable Reasons for Visiting Cyber Cafe by Visitors	No of Respondent		Total
		Yes	No	
1	Speed of Internet	327 (85.2)	57 (14.8)	384 (100)
2	Cost Benefit for Downloading	246 (64.1)	138 (35.9)	384 (100)
3	Help/Assistance	154 (40.1)	230 (59.9)	384 (100)
4	Latest Software	138 (35.9)	246 (64.1)	384 (100)
5	Updated Software	172 (44.8)	212 (55.2)	384 (100)
6	Overall Comfort Level	180 (46.9)	204 (53.1)	384 (100)
7	Price	234 (60.9)	150 (39.1)	384 (100)
Total		1451	1237	
Average Percentage		53.98	46.02	

Figures in bracket indicates Percentages

Graph 5.18 Reasons to visiting a CyberCafe Visitors



From the Graph 5.18 it is clear that Visitors visit Cyber Cafe for many reasons. 85.20 percent of the respondents visit cyber cafe for speed of internet followed by cost benefit for downloading and price with 64.10 percent respondents and 60.90 percent respondents respectively. Other reasons to visit cyber cafe such as assistance, comfort, latest and updated software.

5.8.3 Activities done by Visitors in the Cyber Cafe

Visitors come to Cyber Cafe for performing many activities. From the Table No. 5.23 it can be seen that maximum Visitors come for checking and sending Email which forms 87.80 percent respondents followed by 78.10 percent respondents who come for accessing social net working sites. These two activities are mainly done by the respondents. 49.70 percent respondents agreed that they visit cafe for learning new things followed by 31.30 percent respondents use Cafe for shopping, 28.10

percent use E-governance services from Cafe, 57 percent respondents use Cafe for chatting purpose, 52.10 percent respondents use it for playing games, 70.10 respondents percent use Cafe for downloading various materials, 35.40 percent respondents use it for Net banking, 74.20 percent respondents use it for printing purpose, 34.60 percent respondents use it for CD/DVD Writing or Data copying, 22.70 percent respondents get software coaching from Cafe, 65.90 percent respondents also use Cafe for scanning followed by 34.90 percent respondents use Cafe for getting documents laminated.

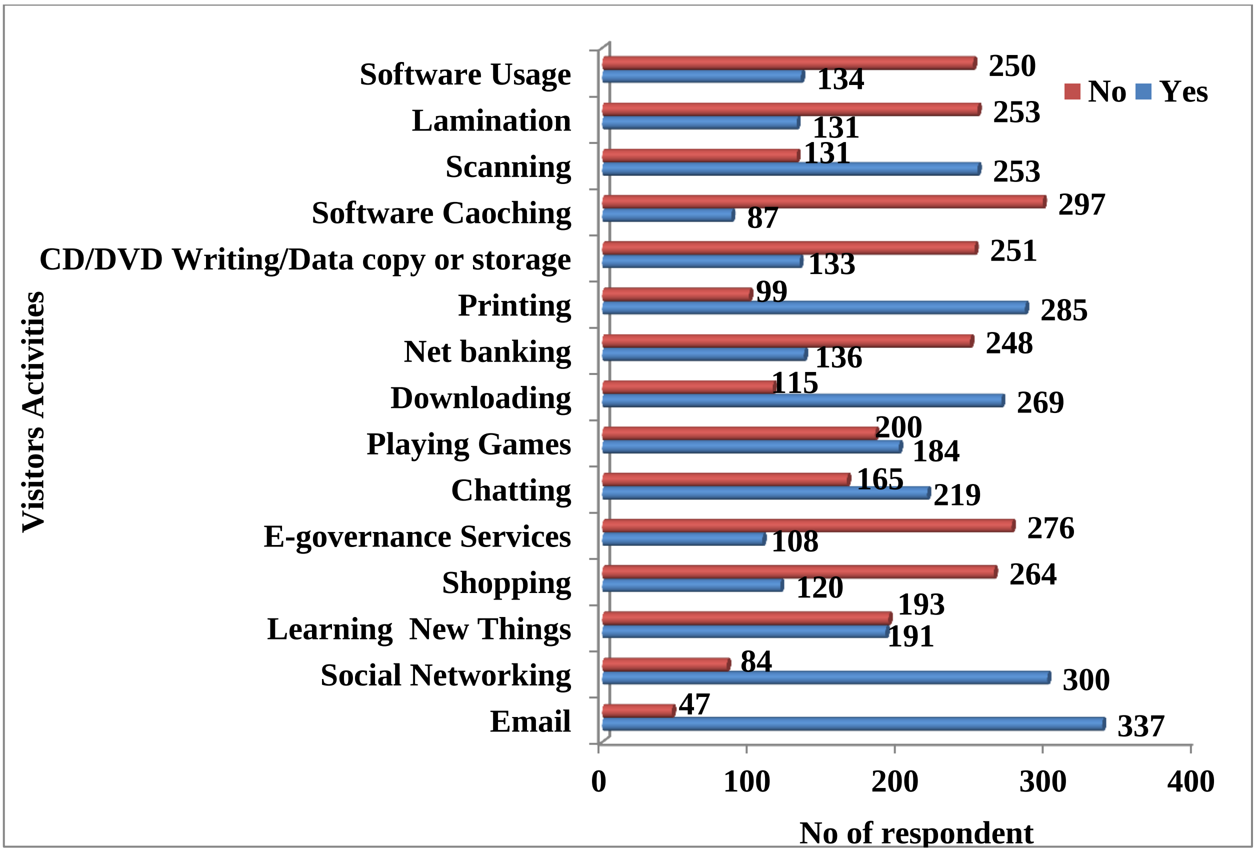
Thus most of the Visitors use Cafe for social networking purpose and email. Printing and scanning are also done by Visitors with a percent of 74.20 percent respondents and 65.90 percent respondent percent respectively. Activities such as chatting with 57 percent, online playing of games with 52 percent respondents, Downloading with 70 percent, net banking with 35.4 percent followed by 30.70 percent respondents doing online shopping, 22.7 percent respondents doing data copying, 65.90 percent respondents do scanning and 34.10 percent respondents get lamination done followed by 34.90 percent respondents use software available in Cyber Cafe. Thus it is clear that respondents visit cyber cafe mainly for accessing social networking sites chatting, downloading and printing as compared to the other activities.

Table No.5.23: Activities Done In Cyber Cafe by Visitors

Sr. No	Activities done in Cyber Cafe by Visitors	No of Respondent		Total
		Yes	No	
1	Email	337 (87.80)	47 (12.20)	384 (100)
2	Social Networking	300 (78.10)	84 (21.90)	384 (100)
3	Learning New Things	191 (49.70)	193 (50.30)	384 (100)
4	Shopping	120 (31.30)	264 (68.80)	384 (100)
5	E-governance Services	108 (28.10)	276 (71.90)	384 (100)
6	Chatting	219 (57)	165 (43)	384 (100)
7	Playing Games	200 (52.10)	184 (47.90)	384 (100)
8	Downloading	269 (70.10)	115 (29.90)	384 (100)
9	Net banking	136 (35.40)	248 (64.60)	384 (100)
10	Printing	285 (74.20)	99 (25.80)	384 (100)
11	CD/DVD Writing/ Data copy or storage	133 (34.6)	251 (65.4)	384 (100)
12	Software Coaching	87 (22.7)	297 (77.3)	384 (100)
13	Scanning	253 (65.90)	131 (34.10)	384 (100)
14	Lamination	131 (34.10)	253 (65.90)	384 (100)
15	Software Usage	134 (34.90)	250 (65.10)	384 (100)

Figures in bracket indicates Percentages

Graph 5.19Activities Done In Cyber Cafe by Visitors



The Graph 5.19 clearly indicates that most of the respondents visit Cyber Cafe for many reasons out of which mainly are social networking, chatting, downloading and Printing. It is also seen 35.40 percent respondents use Cafe for net banking which is important criteria to be considered while considering Cyber security. Other activities such as playing games, chatting, scanning etc. are also done.

5.8.4. Summary

Most of the Visitors visiting the Cyber Cafe are between the age group 16 to 25 years. It is observed that most of the respondents visit Cyber Cafe weekly for many purposes mainly accessing social Networking, playing games, checking mail, downloading, chatting etc. Most of the Visitors mentioned reasons such as they get updated and Latest Software to use, another reason is the price they have to pay is less also the speed of internet that they get is good so they agreed that in cyber cafe by paying low price they get fast internet access.

5.9 Awareness of Cyber Cafe Visitors regarding Cyber security Management:

Visitors should provide documents for identification purpose as per the rules and regulation laid down by the government. Table No.5.24 shows that 60.40 percent respondents show Pan card for ID proof, 53.40 percent respondents show voter card as ID proof, 71.90 percent respondents show student Educational ID proof which is maximum since most of the Visitors are students, 28.90 percent respondents show Employee ID card followed by 17.20 percent respondents show photo credit card, 38.50 percent respondents show UID and 66.40 percent respondents show driving license. Thus it is clear that respondents are aware of the identification process. Student educational ID and driving license are most widely used ID proof used by respondents for identification process. It is seen that 48.10 percent respondents show different documents for identification purpose which can help in future to trace Cyber-criminal in case it happens.

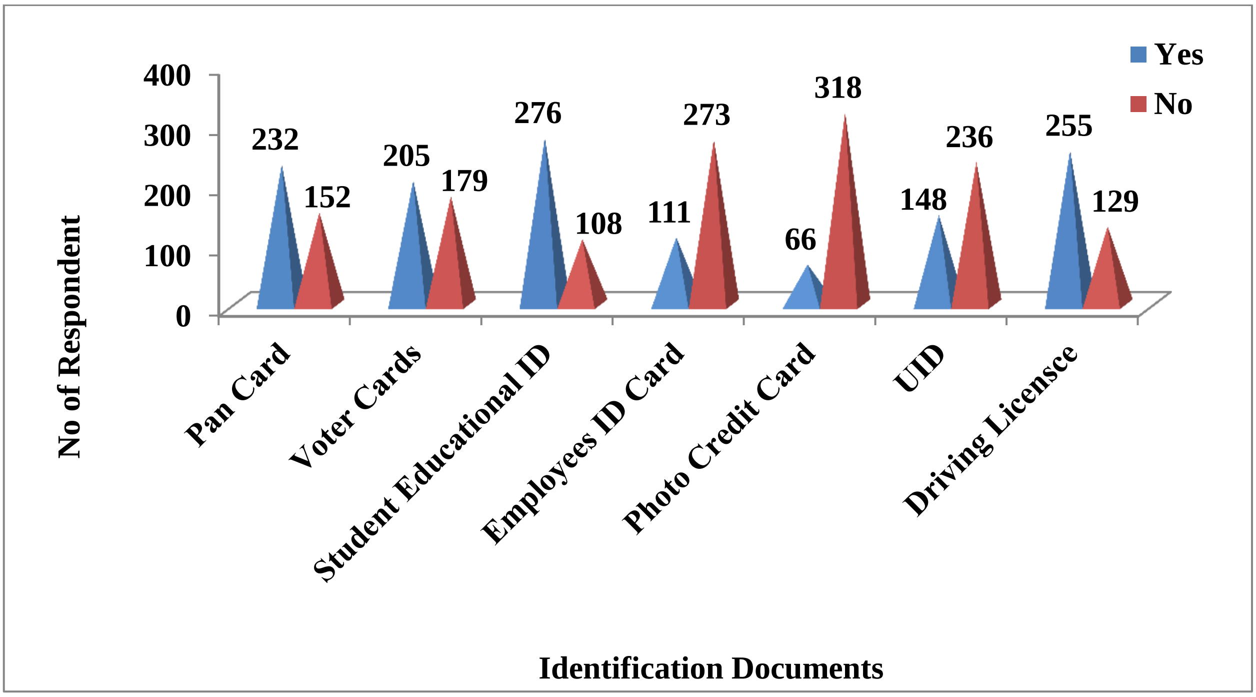
Table: 5.24 Identification Documents

Sr. No	Documents for Identification Purpose	No of Respondent		Total
		Yes	No	
1	Pan Card	232 (60.40)	152 (39.60)	384 (100)
2	Voter Cards	205 (53.40)	179 (46.60)	384 (100)
3	Student Educational ID	276 (71.90)	108 (28.10)	384 (100)
4	Employees ID Card	111 (28.90)	273 (71.10)	384 (100)
5	Photo Credit Card	66 (17.20)	318 (82.80)	384 (100)
6	UID	148 (38.50)	236 (61.50)	384 (100)
7	Driving License	255 (66.40)	129 (33.60)	384 (100)
Total		1293	1395	
Average percentage		48.10	51.90	

Figures in bracket indicates Percentages

From following Graph No. 5.20, it clearly indicates that most of the respondents use Student Educational ID proof and Driving License for document verification with 71.90 percent respondents and 66.40 percent respondents respectively. Other documents such as pan card, voter's card, employee ID, photo credit card or UID are also used for identification purpose to use Internet service. Thus respondents are aware about document verification process laid down by the government.

Graph 5.20 Identification Documents



5.9.1 Awareness about Cyber security

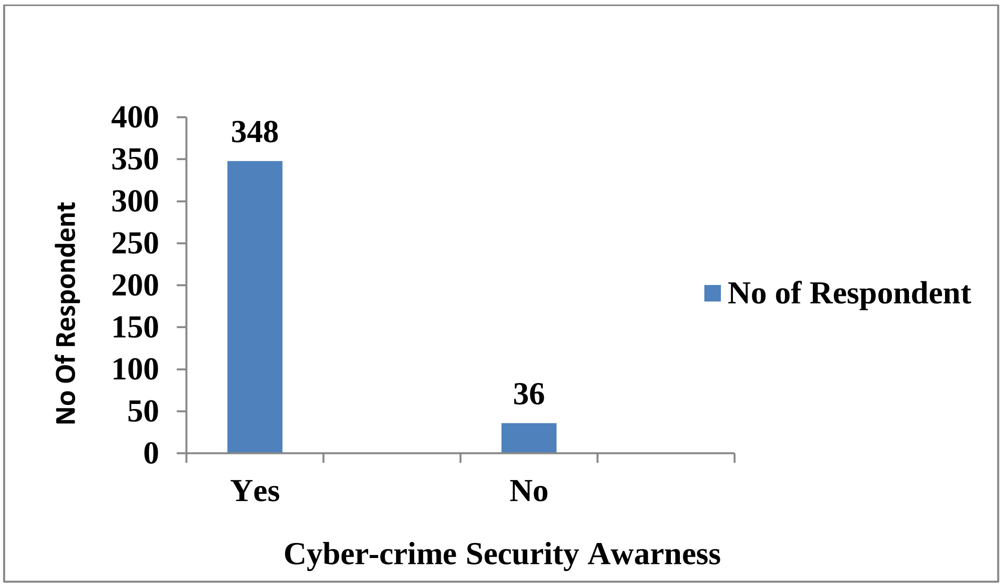
Cyber security awareness is the most important part to avoid Cyber-crime. Visitors must be aware about precautions to be taken to use internet service as well as various types of Cyber-crimes that can take place. From the Table No.5.25 it is seen that 90.62 percent respondents are aware about Cyber security. This is a good sign so that Cyber-crime can be avoided. Only 9.38 percent respondents are not aware about Cyber security.

Table No. 5.25 Cyber Security Awareness

Sr. No	Cyber Security Awareness	No of Respondent
1	Yes	348 (90.62)
2	No	36 (9.38)
Total		384 (100)

Figures in bracket indicates Percentages

Graph 5.21 CyberSecurity Awarness



From the Graph 5.21 it is apparent that most of the respondents are aware about Cyber-crime whereas very few Visitors are not aware about Cyber-crime.

5.9.2 Security Precaution taken by Visitors to Use Internet Services as per Rank:

Most of the Cybercrime occurs due to the negligence of Visitors to consider safety precautions. Visitors must be aware about the security precautions that they should consider when accessing internet services from Cyber Cafe. Table.No.5.26 shows that on average 31.05 percent respondents take cyber security precautions which is very less. 85.90 percent respondents set strong password for their accounts which is ranked first. 78.70 percent respondents does not share personal information with strangers which is ranked second.74.50 percent respondents do not leave computer unattended. 52.20 percent respondents check for use of antivirus or antimalware software.39.60 percent respondents connect with only known person. 26.50 percent respondents checks whether machine has latest update or patches for software which is ranked sixth. 28.70 percent respondents use infrastructure Network only and not using ad-hoc mode and checking encryption security (Wi-Fi). 21.70 percent respondents disable all file sharing which is at 8th rank. 17.20 percent respondents frequently change password. 17.70 percent respondents check if firewall is ON. 15.60 percent respondents make use of private browsing. 25.50 percent respondents avoid financial transactions. 13.10 percent respondents check for browser privacy setting. 13 percent respondents make use of secure web link. 11.70 percent respondents have separate email id for each account.15.90 percent respondents are alert when using cyber cafe internet services. 12.50 percent respondents do not click on unknown link. 8.90 percent respondents agreed that they do not use same password for multiple sites. It is clear that respondents do not take precautions for cyber security while using cyber cafe internet services.68.95 percent respondents are still not taking precautions for cyber security.

Table No. 5.26 Cyber Security Precaution

(Note: Average scale on 1 to 5 (where Strongly Disagree (SD) =1; Disagree (D) =2; Neutral (N) =3; Agree (A) =4; Strongly Agree (SA) = 5))

Security Precaution	SD	D	N	A	SA	Total	Wt. Avg	Rank Order
Setting Strong Password	29 (7.60)	0 0	25 (6.50)	128 (33.30)	202 (52.60)	384	4.22	1
Not Sharing Personal Information With Strangers	22 (5.70)	15 (3.90)	45 (11.70)	119 (31.0)	183 (47.70)	384	4.11	2
Does Not Leave Computer Unattended	27 (7.10)	21 (5.50)	50 (13.10)	139 (36.20)	147 (38.30)	384	3.92	3
Use of antivirus and antispyware /malware software	34 (8.90)	85 (22.20)	65 (16.90)	20 (5.30)	180 (46.90)	384	3.56	4
Connect Only With Known	17 (4.40)	172 (44.80)	43 (11.20)	0 (0)	152 (39.60)	384	3.27	5

People								
Machines has latest patches and updates for S/W	59 (15.40)	121 (31.50)	102 (26.60)	57 (14.80)	45 (11.70)	384	2.66	6
Using infrastructure Network only and not using ad-hoc mode & Checking encryption security(Wi-Fi)	63 (16.40)	153 (39.80)	58 (15.10)	38 (9.90)	72 (18.8)	384	2.64	7
Disable all File Sharing	95 (24.70)	114 (29.70)	92 (24.20)	24 (6.30)	59 (15.40)	384	2.39	8
Frequently Change Password	87 (22.70)	135 (35.20)	96 (250)	22 (5.70)	44 (11.50)	384	2.31	9
Checking Firewall is ON	120 (31.30)	103 (26.80)	93 (24.20)	16 (4.20)	52 (13.50)	384	2.16	10
Make Use Of Private Browsing	100 (26.10)	160 (41.70)	64 (16.70)	5 (1.30)	55 (14.30)	384	2.16	11
Avoid Financial Transactions	150 (39.10)	76 (19.80)	60 (15.60)	58 (15.10)	40 (10.40)	384	2.05	12
Checking Browser Privacy Settings	115 (29.90)	181 (47.10)	38 (9.90)	0 (0)	50 (13.10)	384	1.95	13
Make Use Of Secure Web Link	129 (33.60)	125 (32.60)	80 (20.80)	16 (4.20)	34 (8.80)	384	1.94	14
Separate Email_id	138 (35.90)	142 (37.0)	59 (15.40)	11 (2.9)	34 (8.80)	384	1.82	15
Always Alert	155 (40.40)	126 (32.80)	42 (10.90)	12 (3.10)	49 (12.80)	384	1.80	16
Do not click on unknown links	141 (36.70)	140 (36.50)	55 (14.30)	21 (5.50)	27 (7)	384	1.79	17

Not Using Same Password for Multiple Sites	153 (39.80)	176 (45.80)	21 (5.50)	6 (1.60)	28 (7.30)	384	1.57	18
Total	1634	2045	1088	692	1453			
Average Percentage	23.64	29.57	15.74	10.02	21.03			

Figures in bracket indicates Percentages

5.9.3 Visitors Cyber-crime Awareness as per the Rank

Visitors visiting the cyber cafe should know about different types of Cyber-crimes which will help them to avoid it and protect themselves from cyber-attack. It is seen that the highest average value is 3.9 for the factor ‘Credit Card Fraud’ (75.20 percent) Cyber- crime which the respondents are aware about followed by ‘Hacking’ (78.10 percent) which is 3.8 while ‘Pornography’ (70 percent) is 3.7. Apart from these 72.60 percent respondents are aware about ‘Email Spoofing’ with average value is 3.68, 65.70 percent are aware about ‘Phishing’ with average value 3.46, 61.40 percent respondents are aware about ‘Cyber Stalking’ with average value 3.36 and 40.10 percent respondents are aware about, ‘Intellectual property crimes’ with average value 3.05 and 40.10 percent respondents are aware about internet time theft with an average value of 2.96. Table No. 5.27 shows the ranks of each parameter used to check the awareness about Cyber-crime of Visitors. ‘Credit Card Fraud’ ranks *first* followed by ‘Hacking’. It is seen that 63.52 percent respondents are aware about Cyber-crime awareness.

Table No. 5.27 Cyber-crime Awareness

Cyber-crime Awareness	SD	D	N	A	SA	Total	Wt.Avg	Wt.Avg. (Likert Scale)	Rank Order
Credit Card Fraud	47 (12.30)	11 (2.90)	37 (9.60)	113 (29.40)	176 (45.80)	384	3.90	4.44	1
Hacking	73 (19.0)	11 (2.90)	0 (0)	119 (31.0)	181 (47.10)	384	3.80	4.66	2
Pornography	63 (16.40)	11 (2.90)	41 (10.70)	98 (25.50)	171 (44.50)	384	3.70	4.5	3
Email Spoofing	78 (20.30)	6 (1.60)	21 (5.50)	133 (34.60)	146 (38.0)	384	3.68	4.52	4
Phishing	74 (19.20)	21 (5.50)	37 (9.60)	155 (40.40)	97 (25.30)	384	3.46	4.34	5
Cyber Stalking	84 (21.90)	5 (1.30)	59 (15.40)	158 (41.10)	78 (20.30)	384	3.36	4.26	6
Intellectual Property Crimes	95 (24.70)	35 (9.10)	81 (21.10)	101 (26.30)	72 (18.80)	384	3.05	4.22	7
Internet Time Theft	85 (22.20)	62 (16.10)	83 (21.60)	88 (22.90)	66 (17.20)	384	2.96	4.17	8
Total	599	162	359	965	987				
Average Percentage	19.50	5.29	11.69	31.40	32.12				

Figures in bracket indicates Percentages

(Note:Average scale on 1 to 5 (where Strongly Disagree (SD) =1; Disagree (D) =2; Neutral (N) =3; Agree (A) =4; Strongly Agree (SA) = 5))

5.9.4 Cyber-crime Complaint Registration Awareness

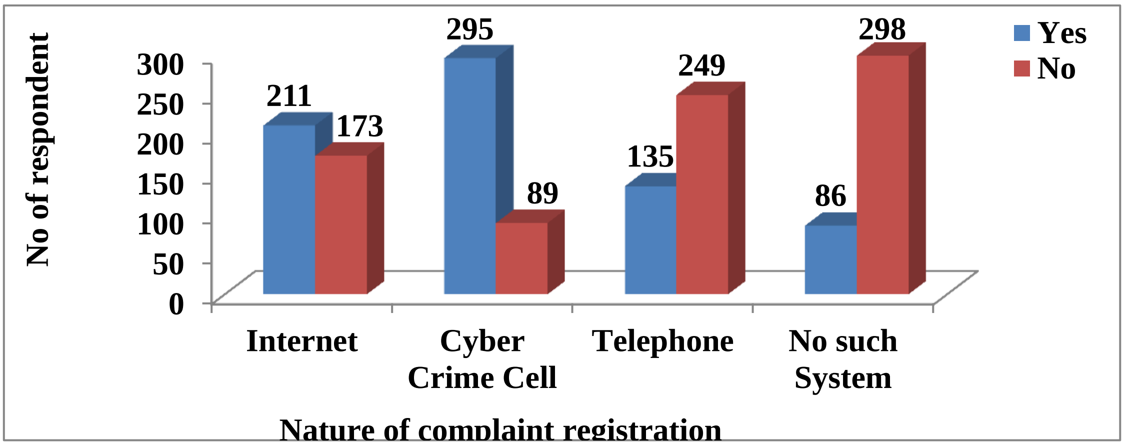
In case a crime occurs Visitors are supposed to register the crime by visiting the Cyber-crime cell. Table 5.28 shows that 55 percent respondents feel that internet can be used for registering the complaint followed by 76.80 percent respondents feel that to register a complaint Cyber-crime cell should be visited which is the correct mean of registering the Cyber-crime complaint.35.20 percent respondents feel that complaint can be registered through Telephone and 22.40 percent respondents feel that there does not exist such system which means they are not aware about the registration process.

Table No. 5.28 Nature of Complaint Registration

Sr. No	Nature of complaint Registration	No of Respondent		Total
		Yes	No	
1	Internet	211 (55)	173 (45)	384
2	Cyber-crime Cell	295 (76.80)	89 (23.20)	384
3	Telephone	135 (35.20)	249 (64.80)	384
4	No such System	86 (22.4)	298 (77.6)	384

Figures in bracket indicates Percentages

Graph 5.22 Nature of Complaint Registration



From the Graph 5.22 it is clear that most of the respondents are aware that they have to register a complaint in Cyber-crime cell in case a crime incident occurs. Still there are Visitors who feel that no such systems of registering the Cyber-crime exist. This is because they are not aware about it. The awareness can be increased if people are made aware about Cyber security and Cyber-crime through news paper, training in institutes and organization.

5.9.5 Cyber-crime Registration Place Awareness

In case a crime occurs the Visitors should visit the police station to register complaint and write an application to the Cyber-crime cell. From the Table No.5.29 it is clear that highest average value is 3.91 for police station with a 74.20 percent followed by Cyber-crime cell which has average value 4.76 and 64.30 percent. This means that most of the respondents are aware about place of registration for Cyber-crime registration. There are few respondents with an average weight of 2.33 who feel a private detective need to be hired with 28.10 percent. Further respondents with 2.02 average weights feels that Cyber-crime can be registered with Loknyalay. Thus it is clear that they are not aware about Cyber-crime registration.

Table No. 5.29 Complaint Registration Place

Complaint Registration Place	SD	D	N	A	SA	Total	Wt.Avg	Wt.Avg. (Likert Scale)	Rank Order
Police Station	48 (12.5)	11 (2.9)	40 (10.4)	110 (28.6)	175 (45.6)	384	3.91	4.47	1
Cyber-crime Cell	117 (30.5)	0 (0)	20 (5.2)	52 (13.5)	195 (50.8)	384	3.54	4.76	2
Private Detective	179 (46.7)	42 (10.9)	55 (14.3)	71 (18.5)	37 (9.6)	384	2.33	4.41	3
Loknyalay	209 (54.4)	38 (9.9)	76 (19.8)	40 (10.4)	21 (5.5)	384	2.02	4.34	4
Total	553	91	191	273	428				
Average Percentage	36.02	5.93	12.43	17.75	27.87				

Figures in bracket indicates Percentages

(Note: Average scale on 1 to 5 (where Strongly Disagree (SD) =1; Disagree (D) =2; Neutral (N) =3; Agree (A) =4; Strongly Agree (SA) = 5))

5.9.6 Summary

It is observed that Visitors are aware about Cyber security management and its rules and regulations. Most of them show the Identification documents when they visit the Cyber Cafe such as driving license or students ID proof or photo Credit or Debit cards. Visitors are aware about Security precautions to be taken under considerations during their visit to Cyber Cafe such as checking browser privacy settings, setting strong passwords, different passwords for different websites, checking of antivirus and antispyware software's etc .Many Visitors are aware about various Cyber-crimes such as Credit Card fraud, Hacking, Pornography etc. and also the place such as Cyber-crime cell to register the Cyber-crime in case a crime occurs.

5.10 Impact of Cyber Security Rules and Regulations on the usage of Cyber Cafe Services on Cyber Cafe Visitors.

It is observed that Cyber Cafe Visitors hesitate to go to Cyber Cafe due to many reasons. Table No. 5.30. Shows that 66.10 percent respondents with average weight of 3.84 feel hesitated due to identification checking performed at Cyber Cafe. 65.60 percent respondents gave reasons for privacy disturbed and hardware device corrupted due to malicious software which has average weight of 3.65. 70.10 percent respondents feel that there is a Misuse of personal Data with an average weight of 3.6. This means that respondents feel unsecure and hesitate to go to Cyber Cafe because they don't get sufficient privacy and feel that their personal data can be misused. There are respondent with an average weight of 3.54 and 64.4 percent respondents who feel hesitated to visit to Cyber Cafe due to low Cyber security. 64 percent respondents with an average weight of 3.54 feel that there is increase in number of Cyber-crime is one reason they feel hesitated for not using the Cyber Cafe. 61 percent respondents with an average weight 3.51 fear that their log history of access is stored so they feel hesitated to go to Cyber Cafe. 62.5 percent respondents with an average weight of 3.45 fears that there can be loss of their data due to Cyber-crime. 48.4 percent respondents with an average weight of 3.38 hesitate due to web camera installed in the Cyber Cafe. 30.2 percent respondents with an average weight of 3.18 that one reason for hesitation is some website are blocked by government which they want to access. Thus it is observed that respondents hesitate to visit Cyber Cafe for many reasons but mainly fear of Cyber-crime is important reason which should be considered.

Table No. 5.30 Hesitation Reason

Hesitation Reasons	SD	D	N	A	SA	Total	Wt. Avg	Wt.Avg (Likert Scale)	Rank Order
Identification Checking	54 (14.06)	10 (2.61)	66 (17.19)	75 (19.53)	179 (46.61)	384	3.84	4.09	1
Privacy Disturbed	56 (14.58)	15 (3.91)	61 (15.89)	124 (32.29)	128 (33.33)	384	3.65	4.32	2
H/W Device Corrupted Due To Malicious S/W	56 (14.58)	15 (3.91)	61 (15.89)	124 (32.29)	128 (33.33)	384	3.65	4.32	3
Misuse Of Personal Data	59 (15.36)	15 (3.91)	41 (10.68)	142 (36.98)	127 (33.07)	384	3.6	4.37	4
Low Cyber Security	60 (15.63)	20 (5.21)	57 (14.84)	145 (37.76)	102 (26.56)	384	3.54	4.27	5
Increase In Number Of Cyber-crime	45 (11.72)	45 (11.72)	48 (12.5)	146 (38.02)	100 (26.04)	384	3.54	4.25	6
Storing Website History	65 (16.93)	5 (1.3)	80 (20.83)	135 (35.16)	99 (25.78)	384	3.51	4.21	7
Data Loss	56 (14.58)	40 (10.42)	48 (12.5)	155 (40.36)	85 (22.14)	384	3.45	4.23	8
Web Camera	46 (11.98)	22 (5.73)	130 (33.85)	111 (28.91)	75 (19.53)	384	3.38	3.97	9
Blockage Of Website By Government	56 (14.58)	49 (12.76)	125 (32.56)	77 (20.05)	77 (20.05)	384	3.18	4.02	10
Total	553	236	717	1234	1100				
Average percentage	14.4	6.15	18.67	32.14	28.64				

Figures in bracket indicates Percentages

(Note:Average scale on 1 to 5 (where Strongly Disagree (SD) =1; Disagree (D) =2; Neutral (N) =3; Agree (A) =4; Strongly Agree (SA) = 5))

5.10.1 Summary

It is seen that most of the Visitors are aware about Cyber-crimes but they feel that their privacy is disturbed due to rules and regulations imposed by the government. The cyber cafe Owners checks the reposndents identification proofs, accssed website history is stored, some websites are blocked by the government and many have installed Web Camera which records their activity. Visitors hesitate to visit cyber cafe since they are not sure about misuse of personal data and also due to increase in Cyber-crime and lack of cyber security in cyber cafe.

5.11 Cost Benefit Analysis of Cyber Cafe in Pune City

Cost Benefit Analysis technique helps for assessing the monetary costs and benefits of a capital investment for Cyber Cafe over a given time period. Cost Benefit Analysis focus on various cost factors and investment for Cyber Cafe. The main goal of any business is to make profit by providing services. Cyber Cafe Owners make profit by provide Internet services to Cyber Cafe Visitors along with that many Owners try to provide a good environment where they can get good bandwidth and availability of uninterrupted electricity, updated software, antivirus and anti-spyware software, scanning and printing facilities, in general a social environment, that provides services, will serve to attract customers.

Table No.5.31 shows the Cost Benefit Analysis for Cyber Cafe. To calculate the profit, factors such as onetime cost which includes Software Cost, Hardware Cost and Infrastructure Cost, annual maintenance Cost, fees per hour for Visitors, total Visitors per day and miscellaneous Income daily were considered.

1. The software cost
   - Operating System software
   - Antivirus
   - Application Software
2. The Hardware cost includes cost
   - Computers
   - Printers &Scanner
   - Any other hardware (Router, Modem, Speakers, Headphones etc.)
3. The Infrastructure cost includes
   - Computer tables
   - Chairs
   - Desk
4. Other cost includes
   - Hardware & Software Maintenance
   - License Renewal, Internet Subscription
   - Electricity bill
   - Rent, Deposit ,Interest on Deposit
   - Operator or staff Charges
   - Depreciation Cost of Hardware and software.

Table No. 5.31 Cost Benefit Analysis of Cyber Cafe

INCOME		EXPENDITURE		
Source of Income	**Amount in Rs.**	**Sources of Expenditure**	**One time charges in Rs.**	**Amount in Rs.**
Internet Access Collection 60 (Visitors/Day) * Rs.20 (Internet Access Cost/hour) * 30 (Days) * 12 (Months).	432000	**Non – Recurring**		
Printing Collection (Rs.200 per day *30 Days/month *12 months)	72000	Chair, Table, Hub, Switches, cables etc.	15000	
Scanning Collection (Rs.100 per day *30 Days/month*12 months)	36000	Computer (10 computers*20000)	200000	
Stationary Sold Collection (Rs.250 per day *30 Days/month*12 months)	90000	Software	20000	
Assistance in the form of Form filling, support, CD / DVD Writing Collection (Rs.50 *30 Days/month*12 months)	18000	Scanner	3000	
Photo coping Collection (Rs.300 per day * 30 Days/month*12 months)	108000	Printer	9000	
Asset Interest Cost (14 % cost of(Chair, Table, Hub, Computer, Scanner, Printer and other hardware and Software))	35980	Any other hardware	10000	
		Deposit	75000	
		Total	**332000**	
		Recurring		
		License		50000
		Internet Subscription		48000
		Electricity Bill		60000
		Rent for space		120000
		Interest on deposit (8.5%)		6375
		Operator Charges		96000
		Hardware and Software Maintenance		4000
		Software Renewal/Subscription		4000
		Depreciation cost (33%) (Chair Table, computer scanner, printer and other Hardware and Software)	84810	
Yearly Expenditure			**Total**	473185
Total Income	791980			
Net Profit (Total Income - Expenditure) (791980-(332000+473185))			**-13205**	

For cost Benefit Analysis for cyber cafe total yearly income and yearly expenditure were considered. On an average 10 computers per cyber cafe, Rs.20 Per hour fees for internet service and 60 Visitors visit cyber cafe per day were considered.

For income various factors such as Internet access Collection, Printing, Scanning, Stationary sold, Assistance provided, Cd/DVD writing collection, Photocopying and 14 % Interest on assets (Chair Table, Computer, Scanner, Printer and Other Hardware such as Modem, Router, Speakers, Headphones etc. and Software) were considered. For first year the total income was calculated to be **Rs. 791980**/-.

For expenditure, cost Recurring and Non-Recurring items were considered. In Non-Recurring cost of Chair Table, Computer, Scanner, Printer and other Hardware required was considered. The total cost of Non-Recurring expenditure for first year was **Rs.332000/-**. For Recurring expenditure factors considered were License ,internet Subscription, electricity bill, rent for space, interest on deposit, operator /staff charges, hardware and software maintenance, software renewal or subscription, and 33% Depreciation cost of asset (Chair Table, Computer ,Scanner, Printer And Other Hardware such as Modem, Router, Speakers, Headphones etc. and Software) were considered.

The total cost of Recurring expenditure for first year was **Rs.473185**/-. It is seen that for the first year there will be a loss of **Rs.13205**/- and profit can be earned from second year.

5.12 Testing of Hypotheses

The method of testing the hypotheses has been described in Para 2.8 earlier. As explained there, many of the statistical tools used for generalization cannot be used in this study to test the hypotheses. If the replies of a majority of the respondents support a hypothesis then that hypothesis will be considered as confirmed. Otherwise it will be considered as rejected. The data connected with the hypothesis and obtained from respondents has been used for this purpose. Conclusions of earlier studies made elsewhere may also be used to supplement the hypotheses of the study.

The following hypotheses have been tested based on the available data:

$H_{1:}$ “Cyber Cafe Visitors are aware about Cyber security and fall short to take precautions to avoid Cyber-crime.”

H_2. “The Cyber Cafe rules and regulations have adversely affected Cyber Cafe.”

H_3. “Cyber Cafe Owners feel that there is a lacuna in the audit done”

5.12.1 Hypothesis 1

The first hypothesis of the study is **“**Cyber Cafe Visitors are aware about Cyber security and fall short to take precautions to avoid Cyber-crime**”**

H_0 Null Hypothesis: Cyber Cafe Visitors are aware about Cyber security and take precautions to avoid Cyber-crime.

H_1 Alternate Hypothesis: Cyber Cafe Visitors are aware about Cyber security and fall short to take precautions to avoid Cyber-crime.

This hypothesis has been tested by using the awareness of Cyber Cafe Visitors regarding Cyber Security and precautions they take to avoid Cyber-crime. To study the awareness and precaution factors, factor analysis is used to develop concise multiple item scales for measuring various constructs. (Table No. 5.26).This test is carried out by using Barletts test of Sphericity which checks the determinant of correlation matrix into consideration which converts it into a chi-square statistics. Another condition needs to be fulfilled before factor analysis would be carried out Kaiser –Meyer-Olkin (KMO) statistics. Hence Hypothesis of the study “Cyber Cafe Visitors are aware about Cyber security and fall short to take precautions to avoid Cyber-crime” is accepted.

Table No. 5.32 KMO and Bartlett's Test Statistics

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.691
Bartlett's Test of Sphericity	Approx. Chi-Square	3314.757
	Df	171
	Sig.	.000

- From above table it is noted that the value of KMO statistics is .691 >0.5, indicating that factor analysis could be used for the given set of data.
- The sample size of study 384 is more than 5 times the number of variables (19).
- Bartlett's Test of Sphericity testing for the significance of correlation matrix of the variables indicates that the correlation coefficient matrix is significant as indicated by p value corresponding to the chi-square statistics. From the above table p value is .000 which is less than 0.05 hence rejecting the null hypothesis and accepts the hypothesis of the study that is “Cyber Cafe Visitors are aware about Cyber security and fall short to take precautions to avoid Cyber-crime”.

5.12.2 Hypothesis 2

Second hypothesis of study is “The Cyber Cafe rules and regulations have adversely affected Cyber Cafe”

H_0 Null Hypothesis: 75% or more Owners agreed that Cyber Cafe rules and regulations have adversely affected Cyber Cafe.(H_0: p = .75)

H_1 Alternate Hypothesis: < 75% Owners agreed that Cyber Cafe rules and regulations have adversely affected Cyber Cafe. (H_1= p < .75)

This hypothesis has been tested by using the primary data collected from Owners regarding the rules and regulations followed in Cyber Cafe and their effect on Cyber Cafe business. To study the adverse effect of rules and regulations of Cyber Cafe, the parameters such as maintaining log registers, type of cubicle and its height, electronically maintained records, document verification, web camera etc. were considered. It is seen that the majority of the Owners (75.37 percent) agreed that Cafe rules and regulations have adversely affected Cyber Cafe (Table No. 5.18).

Table No. 5.33 Z – Statistics for Adverse Effect of Rules and Regulations

Respondents	Sample size	Proportion	Standard error	z - statistic
Owners	134	0.7537	3.7406	0.2005

5% level of significance

As the sample sizes are >= 30 therefore normal approximation is satisfied. In this case Z-test and as one proportion is involved (Refer Para 2.10). Z statistics of awareness of Cyber security is 0.2005 which is < 1.64, hence accept Null hypothesis at 5% level of significance. It means that "The Cyber Cafe rules and regulations have adversely affected Cyber Cafe" and hence the hypothesis of the study is accepted.

5.12.3 Hypothesis 3

Third hypothesis of the study is **"**Cyber cafe Owners feel that there is a lacuna in the audit done**"**

H_0: Cyber Cafe Owners feel that there is a lacuna in the audit done (H_0: p = .65)

H_1: Cyber Cafe Owners feel that there is no lacuna in the audit done (H_1: p < .65)

This hypothesis has been tested by using the primary data collected from Owners regarding the audit done in Cyber Cafe by government official. It is seen that in majority of the Cyber Cafe (64.92 percent) audit is not done as per the response from Owners. (Table No. 5.19).

Table No. 5.34 Z – Statistics of Security Audit Done

Respondents	Sample size	Proportion	Standard error	z - statistic
Owners	134	0.3507	4.1206	0.01698

5% level of significance

As the sample sizes are >= 30 therefore normal approximations are satisfied. In this case Z-test and as one proportion is involved (Refer Para 2.8). Z statistics of audit for Cyber Cafe 0.01698 which is < 1.64, hence accept Null hypothesis at 5% level of significance It is seen that audit is not done for various log sources as per the government guidelines and there are problems in the audit method and thus the hypothesis “Cyber cafe Owners feel that there is a lacuna in the audit done” of the study is accepted.

CHAPTER 6
OBSERVATION AND FINDINGS

6.1 Introduction

This chapter presents the findings of the study. Next the conclusion and suggestion arising out of the study are presented. It was observed during the course of the study that published research material on the subject of the study was strictly limited and a number of areas and aspects require wider and in-depth research in future. The scope for future research is therefore briefly discussed before concluding the chapter. For ready reference and convenience, referent table numbers of the study are given in brackets in the concerned paragraph of the chapter.

6.2 Observations and Findings

The observations and findings set forth in the following pages constitute a recapitulation in a short form of what has been attempted at length in earlier chapters. This study mainly relates to the cyber security management at Cyber Cafe. It considers awareness of Owners and Visitors about cyber security and Cyber-crime. It also considers implementation of cyber security at various levels such as operational level, physical level, application level, database level and network level. The study finds the problems faced by Cyber Cafe Owners for implementing cyber security at Cyber Cafe along with the hesitation reasons of Visitors for visiting Cyber Cafe. The rules and regulation for Cyber Cafe are followed or not are observed in the study. Four objectives and three hypotheses lay primary emphasis on this subject. All objectives focus on cyber security management system, cyber-crime and security awareness, impact of rules and regulation for Cyber Cafe on Owners and Visitors. The researcher of this study has considered cyber security for Cyber Cafe at national and international level. This unique approach has provided new insights, added to the important conclusions and enriched this study. The researcher has analyzed the primary data to study the cyber security implemented in Cyber Cafe, problems with respect to cyber security to Owners and Visitors, designs and development of effective security system framework for Cyber Cafe. Owners view about cyber security management is presented in Part I, Visitors view about cyber security management is presented in part II.

6.2.1 Part I: Cyber Cafe Owners

➢ The Owners background with respect to their education, computer literacy and Cyber security management knowledge is found out. Problems faced by the Owners while running the Cyber Cafe are identified such as lack of assistance in case a Cyber-crime occurs, High maintenance cost, Lack of indicators in case an attack of Cyber-crime is under way and many others. Awareness about Cyber-crime among Owners is also identified.

- Considering the education background it is observed that most of the Cyber Cafe Owners are graduates followed by Higher Secondary, Post Graduates and above and then secondary.(Table No.5.4)
- In terms of computer background it is seen that 50 percent Cyber Cafe Owners have done professional certification and short term course followed by computer diploma and computer degree.(Table No.5.5)
- On an average 60.44 percent Cyber Cafe Owners agree that different types of problems are faced by them. 65.60 percent say that Reputation is Hampered due to government rules and regulation followed by 25.40 percent says that they have to bear High Maintenance cost, 73.90 percent say that there is Lack of indicators in case an Cyber-crime attack is going to take place, 59.70 percent agree that they Lack knowledge about security maintenance, 66.4

percent feel that there is Lack of established resources to know about cyber security updates. (Table No.5.6)

- 98.50 percent Owners has broad brand connection type where as 17.16 percent Owners use broad band Wi-Fi and nobody use dial up connection. (Table No.5.7)
- It is revealed that on an average awareness about Cyber-crime of Owners was 58.22 percent. Of concern 69.40 percent Owners are aware about cyber pornography, 59.0 percent are aware about Intellectual Property crime, 54.50 percent Owners are aware about Money Laundering Evasion, 61.20 percent Owners are aware about Electronic Fund Transfer, 68.7 percent Owners are aware about Hacking, 58.20 percent Owners are aware about Email spoofing followed by 51.50 percent Owners aware about political spoofing, 53.70 percent Owners are aware about Electronic Terrorism and 47.80 percent Owners are aware about E-murder. (Table No.5.8)

➢ The awareness of cyber security management among Owners is found out by finding how they implement cyber security and mange it. Different factors are taken into considerations such as technical security techniques used to implement cyber security, physical security techniques, the level at which security is maintained and type of internet connection used.

- Most of the Owners implement Cyber security by self method that is 85.07 percent whereas 14.93 percent make use of Automated method. 30.60 percent respondents implements cyber security at End Point level, out of which 23.88 percent respondents make use of Self method and 6.72 percent respondents make use of automated method. 66.42 percent respondents implements cyber security at Gateway level, out of which 59.70 percent respondents make use of Self method and 6.72 percent respondents make use of automated method. 2.98 percent respondent's implements cyber security at Both level, out of which 1.49 percent respondents make use of Self method and automated method. (Table No.5.9)

- It is observed that on an average 49.58 percent Cyber Cafe Owners are aware about cyber security techniques to be used to avoid Cyber-crimes and have apparently implemented them in their Cyber Cafe. 96.30 percent Owners used antivirus software as security techniques, 44.50 percent Owners say that they have End Point security software installed and 58.20 percent Owners used antispyware software. 76.90 percent Owners had Firewall settings done which is available default with operating system. 63.40 percent used Network access control so that required access to network can be given only when needed. 50 percent Owners restrict access to the control panel followed by 38.80 percent Owners restricts changes in browser security. 47.80 percent Owners restrict access to physical drives. 57.50 percent Owners changed the router username and password frequently so that it is not hacked. 38.10 percent Owners blocked the setup files and automatic installation of software without Owners concern. 13.40 percent Owners have installed Unified Threat Management Device (UTM) and UTM software which protects from many cyber vulnerabilities. 42.50 percent Owners used website keyword blocking mechanism by using antispyware or antivirus software or through service provider by default and are aware about this feature. 26.10 percent Owners used content filter to filter out unwanted request from Visitors. (Table No.5.10 - A)
- On an average 7.66 percent Owners are aware about Cyber Security techniques to be used when making use of connection Type Wi-Fi to avoid Cyber-crime.11.19 percent Owners Turn off Wireless Router manually, 3.74 percent Owners change Username and Password of access point, 9.71 percent Owners disable auto connect mode, 7.47 percent Owners shutdown access point, 17.70 percent Owners place wireless router inside building, 3.74 percent Owners disable DHCP service, 4.47 percent Owners make use of

WPA protocol, 4.47 percent Owners make use of TKIP protocol, 3.74 percent make use of WEP and WPA2 protocol, 9.71 percent Owners store MAC address, 7.47 percent Owners use filter MAC address and14.18 percent block anonymous IP address. (Table No.5.10 - B)

- On an average 7.58 percent Owners implement physical cyber security techniques. 20.90 percent of Owners locks windows so that theft cannot take place. Apart from these Owners used various techniques like locking of PC cases or using alarm sensors on routers and break glass alarms or detectors etc. 8.20 percent Owners have separate server room for servers in Cyber Cafe. (Table No.5.11)

- ➢ The awareness about Cyber Cafe rules and regulation among Owners is found out using various factors such as prevention provision, log maintenance such as computer access record, History of websites access and, mail server log, Firewall or Intrusion Prevention /Detection Log, checking and verifying identification of Visitors, infrastructure rules such as cubicle height, type of cubicle and audit done for Cyber Cafe. Usage of banned software is also found out. Details regarding Electronic log of mapping with masqueraded IP address is maintained or not is identified.
  - It is observed that 91.53 percent Owners have provision for Cyber-crime prevention. 94.0 percent Owners display rules for accessing Cyber Cafe, 92.50 percent display poster for restricted website and 88.10 Owners display government rules for Cyber Cafe. (Table No.5.12)
  - On an average 44.68 percent Owners Cyber Cafe maintains logs for Cyber Cafe activities and resources used. 94 percent of Owners maintain users log register that consist of their identification proof and other details.
  - 51.50 percent Owners have web camera installed and 71.60 percent Owners have fire extinguisher for safety.

- 30.60 percent Owners maintain computer access record along with 27.60 percent Owners maintain History of websites accessed using computer resource at Cyber Cafe, 34.30 percent Owners maintain Logs of proxy server installed at Cyber Cafe, 31.30 percent Owners maintain Mail server logs, 45.50 percent Owners maintain Logs of network devices such as router, switches, systems etc. installed at Cyber Cafe and 15.70 percent Owners maintain Logs of firewall or Intrusion Prevention/Detection systems, if installed. (Table No.5.13)
- Visitor’s identification is mandatory part of government rules for which various documents are checked. Thus 100 percent Owners say they allow student educational ID as ID proof, 85.10 percent Owners allow photo Credit Card, 85.80 percent Owners allow UID card as ID proof, 94.80 percent Owners allow Voter ID card followed by 98.5 percent Owners allowing employee ID, 82.80 percent Owners allowing photo Debit card and 97.80 percent Owners allowing Driving License as ID proof. It is seen on an average 92.11 percent of Visitors show various identification document. (Table No.5.14)
- It is observed 91.0 percent Cyber Cafe have open cubicles and 9.0 percent still have closed cubicles.(Table No.5.15)
- 54.50 percent Owners have cubicles or partition height as 4.5 feet and 28.5 percent Cyber Cafe have 3.5 feet height followed by 7.5 percent Cyber Cafe with 2.5 feet height and 2.20 percent Cyber Cafe have 1.5 feet of cubicle height. Only 7.50 percent of Cyber Cafe have cubicle height more than 4.5 feet, (Table No.5.16)
- It is seen on an average that 58.80 percent Owners follow infrastructure and technical rules as per government rules. 41.20 percent Owners still do not follow infrastructure and technical rules. It is observed that 92.50 percent Cyber Cafe have computer machines in Cyber Cafe facing outward. 69.40 percent Cyber Cafe have shared IP address and 56.7 percent Cyber Cafe have

IP mapping with machine. 54.50 percent Owners keep electronic log of mapping with masqueraded IP address and 20.90 percent Owners still use banned software such as Deepfreeze (Table No.5.17)

- 75.37 percent Owners feel that due to the rules and regulations imposed by the government there is a decline in number of Visitors in Cyber Cafe.(Table No.5.18)
- On an average 76.38 percent Owners feels that there is increase in Cyber-crime awareness among Visitors.(Table No.5.18)
- It is observed that only 28.51 percent Owners agree that audit for various log sources are done as per government guidelines. 35.07 percent Owners agree that Audit is done for Cyber Cafe whereas 64.92 percent Owners do not agree to this. 35.07 percent Owners responded that Manual and Online version of Visitors Log Register Audit is done for Cyber Cafe. 26.12 percent Owners responded that System server logs are checked, 15.67 percent Owners agreed that Network audit is done and 30.59 percent Owners responded that Application Security Audit is done. Table No.5.19)

6.2.2 Part II :Cyber Cafe Visitors

- The Visitors age, purpose and frequency of visit to the Cyber Cafe are found out. Different factors for visit such as accessing social networking, playing games, checking mail, downloading, chatting etc. along with updated and Latest Software to use, another reason is the price that Visitors pay and also the speed of internet are considered.
  - It is observed that on an average 57.82 percent Visitor belong to Male category whereas 42.18 percent belong to Female category. (Table No.5.19)
  - On an average 53.63 percent of the Visitors who come to Cyber Cafe are under the age group between 16 to 25 years. (Table No.5.20)
  - It is revealed that 12.0 percent Visitors visit Cyber Cafe on daily basis whereas 29.40 percent visit Cyber Cafe weekly. 19.30 percent visit Cyber

Cafe monthly followed by 2.60 percent visiting Cyber Cafe yearly and 36.70 percent Visitor visiting Cyber Cafe randomly. (Table No.5.21)

- It is seen that there are many reasons for Visitors to visit Cyber Cafe. 85.20 percent Visitors visit Cyber Cafe for speed of internet, 64.10 percent use cafe for cost benefit for downloading, 40.10 percent Visitors visit for Help or assistance, 35.90 percent visit because they can get latest software to use, 44.80 percent visit Cyber Cafe because they can get updated software to use. 46.90 percent use Cyber Cafe because they find it more comfortable followed by 60.90 percent Visitors visit cafe because they feel price that they have to pay is less and affordable. (Table No.5.22)
- It is seen that Visitors use cafe for number of activities. 78.10 percent Visitors visit cafe for social networking purpose. 49.70 percent Visitors visit for learning new things followed by 31.30 percent Visitors use cafe for shopping, 28.10 percent Visitors do E-governance services from cafe, 57 percent Visitors use cafe for chatting purpose, 52.10 percent Visitors use it for playing games, 70.10 percent Visitors use cafe for downloading various materials, 35.4 percent Visitors use it for Net banking, 74.20 percent Visitors use it for printing purpose, 34.60 percent Visitors use it for CD/DVD Writing or Data copying , 22.70 percent Visitors get software coaching from cafe, 65.90 percent Visitors also use cafe for scanning followed by 34.90 percent Visitors use cafe for getting documents laminated. (Table No.5.23)

➢ Visitors awareness about Cyber security management and its rules and regulations is identified by focusing on various factors such as identification and verification of documents such as license or students ID proof or photo Credit or Debit cards. Other factors considered are Security precautions to be taken under considerations during their visit such as checking browser privacy settings, setting strong passwords, different passwords for different websites, checking of antivirus and antispyware software’s etc. Along with this awareness about

Cyber- crime such as Credit Card fraud, Hacking, Pornography etc. and also the awareness of place of complaint registration such as Cyber-crime cell in case a crime occurs are identified.

- It is revealed that on average 48.10 percent Visitors make use of various documents for proving identity of themselves. 60.40 percent Visitors show Pan card for ID proof, 53.40 percent Visitors show voter card as ID proof, 71.90 percent Visitors show student Educational ID proof which is maximum since most of the Visitors are students, 28.90 percent Visitors show Employee ID card followed by 17.20 percent Visitors show photo credit card, 38.50 percent show UID and 66.40 percent Visitors show driving license as Identification Proof. (Table No.5.24)
- It is observed that 90.62 percent Visitors are aware about cyber security where as only few are unaware about cyber security. (Table No.5.25)
- It is found that on an average 31.05 percent Visitor take cyber security precautions during their visit to Cyber Cafe. (Table No.5.26)
- 85.90 percent Visitors set strong password for their accounts which is ranked first. 78.70 percent Visitors do not share personal information with strangers and 74.50 percent Visitors do not leave computer unattended. (Table No.5.26)
- 52.2 percent Visitors check for use of antivirus or antimalware software and 39.60 percent Visitors connect with only known person. (Table No.5.26)
- It is found that 26.50 percent Visitors checks whether machine has latest update or patches for software and 28.70 percent Visitors use using infrastructure Network only and not using ad hoc mode and checking encryption security (Wi-Fi). (Table No.5.26)
- It is revealed that 21.70 percent Visitors disable all file sharing and 17.20 percent Visitors frequently change password whereas 17.70 percent Visitors check if firewall is ON. (Table No.5.26)

- It is seen that 15.60 percent Visitors make use of private browsing and 25.50 percent Visitors avoid financial transactions. (Table No.5.26)
- It is observed that 13.10 percent Visitors check for browser privacy setting and 13 percent Visitors make use of secure web link. (Table No.5.26)
- It is seen that 11.70 percent Visitors have separate email id for each account and 15.90 percent Visitors are alert when using Cyber Cafe internet services. (Table No.5.26)
- It is observed that 12.50 percent Visitors do not click on unknown link and 8.90 percent Visitors agreed that they do not use same password for multiple sites.
- It is clear that Visitors do not take precautions for cyber security while using Cyber Cafe internet services since on an average 68.95 percent Visitors are still not taking precautions for cyber security (Table No.5.26)
- It is seen that 74.20 percent Visitors are aware about ‘Credit Card Fraud’ with an average weight of 3.9 followed by ‘Hacking’ with a percent of 78.10 which has an average weight of 3.8 while ‘Pornography’ awareness is 70 percent among Visitors and has an average weight of 3.7. Apart from these 72.60 percent Visitors are aware about ‘Email Spoofing’ with an average weight of 3.68, 65.70 percent Visitors are aware about ‘Phishing’ with an average weight of 3.46. (Table No.5.27)
- 61.30 percent Visitors are aware about ‘Cyber Stalking’ with an average weight of 3.36 and 45.10 percent Visitors are aware about ’Intellectual property crimes’ with an average weight of 3.05. 40.10 percent Visitors are aware about ‘Internet Time Theft’ with an average weight of 2.96. (Table No.5.27)
- It is found that 55.0 percent Visitors feel that internet can be used for registering the complaint followed by 76.80 percent feel that to register a complaint Cyber-crime cell should be visited. 35.20 percent Visitors feel that complaint can be registered through Telephone and 22.40 percent Visitors

feel that there does not exist such system which means they are not aware about the registration process.(Table No.5.28)

- It is seen that 45.62 percent Visitors on an average are aware about complaint Registration place. 74.20 percent Visitors feel that complaint should be registered in police station with an average weight of 3.91 followed by Cyber-crime cell which has average weight 4.76 and 64.30 percent. There are few Visitors with an average weight of 2.33 who feel a private detective need to be hired with 28.10 percent followed by 15.90 percent Visitors with an average weight of 2.02 who say Cyber-crime can be registered with Loknayala. (Table No.5.29)

➢ Different hesitation reasons for visiting Cyber Cafe by Visitors are identified. For this, factors such as checking of identification proofs, accessing website history, some websites blocked, and installation of web camera along with it fear of Cyber-crime, misuse of personal data and lack of cyber security are considered.

- It is observed that 66.10 percent Visitors with average weight of 3.84 feel hesitated due to identification checking performed at Cyber Cafe, 65.60 percent Visitors felt their privacy is disturbed and hardware device corrupted due to malicious software which has average weight of 3.65. (Table No.5.30)
- 70.10 percent Visitors feel that there is a Misuse of personal Data with an average weight of 3.6. There are Visitors with an average weight of 3.54 and 64.40 percent who feel hesitated to visit to Cyber Cafe due to low Cyber security. (Table No.5.30)
- On an average 64.0 percent Visitors with an average weight of 3.54 feel that there is increase in number of Cyber-crime is one reason they feel hesitated for not using the Cyber Cafe and 61.0 percent Visitors with an average

weight 3.51 fears that their log history of access is stored so they feel hesitated to go to Cyber Cafe. (Table No.5.30)

- It is observed that 62.50 percent Visitors with an average weight of 3.45 fears that there can be loss of their data due to Cyber-crime and 48.40 percent Visitors with an average weight of 3.38 hesitate due to web camera installed in the Cyber Cafe. (Table No.5.30)
- It is seen that 30.20 percent Visitors with an average weight of 3.18 feel that one reason for hesitation is some website are blocked by government which they want to access. (Table No.5.30)
- It is observed that on an average 59.85 percent Visitors feel hesitated to visit Cyber Cafe for different reasons such as stringent government rules and regulation. (Table No.5.30)

6.2.3 Part III :Cyber Cafe Owners and Visitors

➢ The Cyber Cafe Owners and Visitors awareness about Cyber security, Cyber -crime, Rules and Regulations for cyber cafe is found it. The precautionary methods taken into consideration by both of them to avoid cyber-attack and Cyber-crime are found out. Impact of Rules and regulation among Cyber Cafe Owners and Hesitation reasons of Visitors to visit cyber cafe are studied and observed.

- It is observed that on an average awareness about Cyber-crime of Owners was 58.22 percent and 63.52 percent Visitors are aware about Cyber-crime.(Table 5.8 and 5.27)
- It is observed that on an average 49.58 percent Cyber Cafe Owners are aware about cyber security techniques for Broadband (without Wi-Fi) to be used to avoid Cyber-crimes and have apparently implemented them in their Cyber Cafe and 7.66 percent Owners are aware about Cyber security techniques to be used when making use of connection Type Wi-Fi to avoid Cyber-crime. Where as it is found that on an average 31.05 percent Visitor take cyber

security precautions during their visit to Cyber Cafe. (Table 5.10 - A&B and 5.26)

- It is seen that 75.37 percent Owners feel that due to the rules and regulations imposed by the government there is a decline in number of Visitors in Cyber Cafe. It is observed that on an average 59.85 percent Visitors feel hesitated to visit Cyber Cafe for different reasons.(Table 5.18 and 5.30)
- 92.11 Percent Owners verify ID proof of Visitors and 48.10 percent Visitors agreed that they provide ID proof while using the Cyber Cafe services.(Table 5.14 and 5.24)

CHAPTER 7
CONCLUSIONS, SUGGESTIONS AND SCOPE FOR FURTHER RESEARCH

7.1 Conclusions

This chapter presents the conclusion and suggestion arising out of the study. It was observed during the course of the study that published research material on the subject of the study was strictly limited and a number of areas and aspects require wider and in-depth research in future. The scope for future research is therefore briefly discussed before concluding the chapter. The efforts to combat the new and rising cyber threats through Cyber Cafe so far have been pragmatic.

- ➢ The majority of Owners are graduates and few of them have completed post graduation degree but computer literacy is less. It is seen that very less number of Owners have computer background. Many problems are faced by Owners while running the Cyber Cafe. Cyber Cafe has Broad Band connection and it is observed by the researcher that most of the non-registered Cyber Cafe has Wi-Fi in there Cafe. Owners are also aware about various types of Cyber-crime and security techniques implementation at technical level. At physical level the Owners are not much serious about cyber security implementation. Owners are aware about Broadband connection security techniques but not for Broadband Wi-Fi. The Owners follow the Rules and Regulation for infrastructure and technical details such as log maintenance, use of antivirus software etc. The owner agreed that audit of Cyber Cafe is not done by government officials as per rules and regulations and there are problems in it.
    - Most of the Owners are highly educated and have completed their graduation.

- For better and effective cyber security Computer professional certification or short term computer courses is done by less number of Owners and those who have not done computer course make use of practical experience to operate cafe.
- Awareness of the Cyber security Management depends totally on the Cyber Cafe Owners Education, Computer Background and Internet Literacy Parameter.
- Cyber Cafe Owners faces many problems while running the Cyber Cafe.
- High maintenance cost is needed to maintain the cafe.
- Owners feel that Cyber Cafe reputation is hampered affecting Cyber Cafe business due to the Cyber-crimes taking place through Cyber Cafe.
- Owners find lack of assistance and lack of information from government side in case if a cyber-crime attack takes place.
- Owners feel that there are lacks of established resources to know about cyber security updates.
- Most of the Owners agree that they do not have sufficient knowledge of cyber security maintenance.
- Most of the Owners have Broad Band Internet connection and few of them have started with Wi-Fi Internet Services.
- Most of the Owners are aware about different types of Cyber-crime such as Pornography, Hacking, and Intellectual Property Crime etc. which help them to prevent Cyber-crime and take necessary action when required.
- Cyber Security is mostly maintained at Gateway level and is done by Owners themselves.
- Owners use various techniques to implement cyber security such as installing Antivirus & Antispyware software, installing UTM device, Installing Firewall, Restricting access to Control panels, Browser settings and Physical drives etc.

- Blocking installation and setup files, Techniques such as Remote client monitoring, Content Filtering are also done by Owners to maintain cyber security.
- Less number of owners make use of Wi-Fi security technique such as Turn off Wireless Router Manually, change Username and Password of access point, disable auto connect mode, shutdown access point, place wireless router inside building, disable DHCP service, use of WPA/WEP/TKIP/WEP2 protocol, store MAC address, filter MAC address and block anonymous IP address.
- Owners are not aware and not serious about physical cyber security and very few of them maintain physical cyber security such as locking of PC cases, putting alarm sensors, locking windows and separate server room.
- Most of the Owners take step to prevent Cyber-crime as per the guidelines provided by government by displaying posters indicating Cyber Cafe rules and government rules such as not accessing restricted or pornographic website.
- Majority of the owners are aware about government laid rules and regulations for Cyber Cafe and follow them in their Cyber Cafe.
- Owners maintain log registers for visitors along with log details of web camera, computer access record, history of websites accessed proxy server logs, mail server logs, network devices logs, firewall logs for maintaining cyber security and controlling Cyber-crime.
- As per the government rules Owners strictly check visitors' identification proofs such as Driving license, Voter card, and Student ID card, Photo Credit Card or Debit Card etc.
- As per the Rule of government most of the Owners have open cubicles and the partition is not more than 4.5 feet along with this all machines face outward.

- Owners also maintain logs of mapping with masqueraded IP address, details regarding IP mapping with machine and details of sharing of IP address.
- Most of the Owners do not use banned software which deletes details regarding use of internet service like Deepfreeze software.
- Owners agree that due to the rules and regulations imposed by the government there is decline in Cyber Cafe visitors but on the other hand there is increase in Cyber-crime awareness among visitors also.
- Owners agree that audit is done for various log sources such as system server log , network audit, Application security audit, Manual and Online version of Visitors Log Register as per government guidelines but it is done at less percentage.

➢ Most of the Visitors visiting the Cyber Cafe are between the age group 16 to 25 years. Visitors visit Cyber Cafe weekly for different purposes and reasons such as they get updated and Latest Software to use, another reason is the price they have to pay is less and also the speed of internet that they get is good. Visitors are aware about Cyber security management and its rules and regulations. Visitors are aware about Security precautions to be taken under considerations during their visit to Cyber Cafe but are not serious about it. Many Visitors are aware about various Cyber-crimes and also the place such as Cyber-crime cell to register the Cyber-crime in case a crime occurs. The Visitors hesitate to visit Cyber Cafe mainly due to fear of various reasons such a Cyber-crime, no privacy, fear of identity theft through identification checking etc.

- Male youngsters between the age group 16 to 25 years are frequent visitors to Cyber Cafe.
- Most of the visitors visit Cyber Cafe randomly or weekly while few visit monthly and daily. Very less visitors visit cafe yearly.
- In totality Visitors are satisfied with the Cyber Cafe services as they agree that they get best internet speed, latest and updated software, cost benefit and

overall comfort level by visiting to Cyber Cafe and also they get help or assistance to use internet services.

- Visitors visit Cyber Cafe to use internet services for many activities such as social Networking, Net banking, Shopping Downloading, E-governance services, Chatting, Software usage etc.
- As per the government rules regarding verification of ID, Visitors shows various ID proofs like Student ID card, Driving License, Adhar Card, Voter card etc.
- Most of the Visitors are aware about cyber security.
- Visitors do not take precautions while using internet service in Cyber Cafe by setting strong password as well as different passwords for different accounts. Also they do not take precautions in the form such as to connect to only known people ,check browser security, making use of private browsing, avoid financial transactions, disable file sharing etc.
- Visitors are highly aware about cyber-crime such as Credit Card fraud, Hacking, Pornography, Email Spoofing, Phishing, Cyber Stalking, Intellectual Property Crimes, and Internet Time Theft etc.
- Most of the Visitors are aware about complaint registration process and place of registration.
- Visitors hesitate to visit the Cyber Cafe due to many reasons such as misuse of personal data, their privacy is disturbed, due to less cyber security, identification process makes them feel awkward ,some website that they want to access are blocked due to content filtering etc.

7.2 Designed and Suggested Framework of Cyber Cafe Business Model

Figure 7.1 Cyber Cafe Business Model explains the business view of Cyber Cafe. Cyber Cafe Business provides many services to its visitors out of which they earn profit. Along with profit making the other objectives of the cafe business are providing customer satisfaction, getting more customers, providing quality service and mainly providing a cyber-threat environment. The main service that they offer to the visitors is internet service. The other services that they offer are selling computer accessories, printing, CD\DVD writing, training, and scanning, gaming station etc. For offering these services and running the Cyber Cafe investment in terms of hardware, software, infrastructure maintenance of cafe, labor cost etc. has to be done. The basic problem they face is related to cyber security issues. Problems such as key loggers, malicious code (virus, botnets, worms) pornography, spamming, staking, Hotspot stealing, Hardware problems, theft, Denial of service attack, key loggers, Intrusion, Spoofing and Masquerading, less knowledge of security and auditing, bandwidth problems and many more.

Cyber Cafe Owners and government official along with cyber security expert need to collaborate with each other to define suitable policy with proper planning and risk management. As per the primary data collected it was observed that there is a strong need for security framework for Cyber Cafe and law amendment on regular basis. Researcher provides a security framework for the Cyber Cafe which will guide the stakeholders to implement security for Cyber Cafe. Researcher in this model focuses on various elements to be considered for security management such as Assets, Policy, Security Technology and Planning and Risk management. By making use of Security Framework ($S^2C^23^2$) the confidentiality, integrity and availability of assets can be achieved. The risk based model will help to mitigate risk before their negative impact occurs.

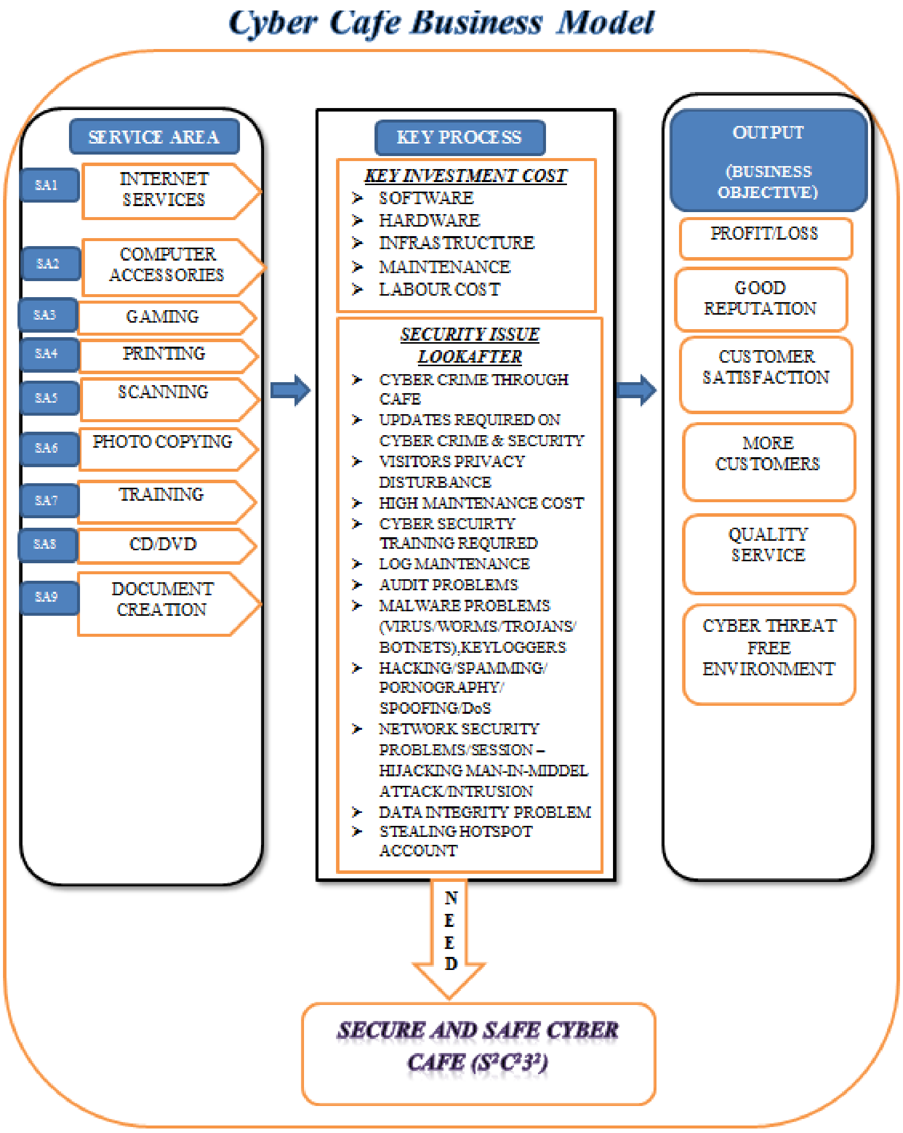


Fig 7.1: Cyber Cafe Business Model

7.3 Security Framework ($S^2C^23^2$)

The Secure and Safe Cyber Cafe security framework ($S^2C^23^2$) provides a framework for successful cyber security management. Fig 7.2 represents the Secure and Safe Cyber Cafe security framework ($S^2C^23^2$). It provides guidance for stakeholders including tools and techniques to understand and manage cyber security risk to business operations. The stakeholders for this model are the Cyber Cafe Owners, Visitors and government officials.

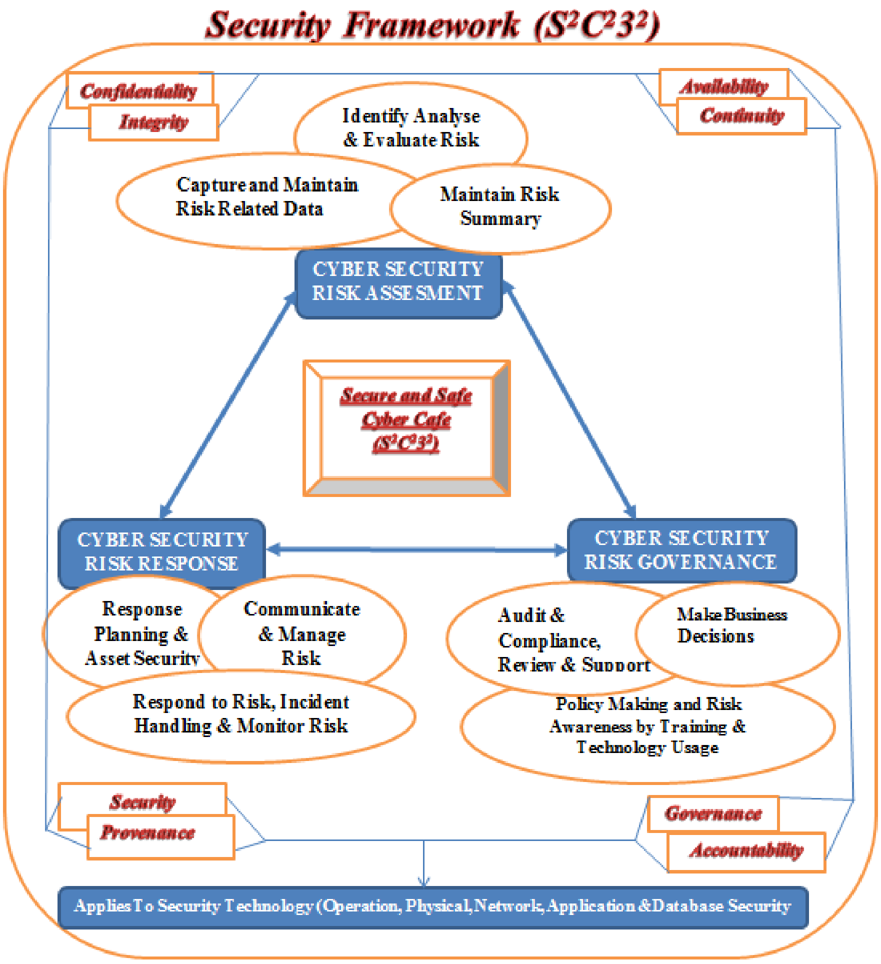

Security Framework (S²C²3²)
Confidentiality
Integrity
Availability
Continuity
Identify Analyse & Evaluate Risk
Capture and Maintain Risk Related Data
Maintain Risk Summary
CYBER SECURITY RISK ASSESMENT
Secure and Safe Cyber Cafe (S²C²3²)
CYBER SECURITY RISK RESPONSE
CYBER SECURITY RISK GOVERNANCE
Response Planning & Asset Security
Communicate & Manage Risk
Respond to Risk, Incident Handling & Monitor Risk
Audit & Compliance, Review & Support
Make Business Decisions
Policy Making and Risk Awareness by Training & Technology Usage
Security
Provenance
Governance
Accountability
Applies To Security Technology (Operation, Physical, Network, Application & Database Security

Fig.7.2: Security Framework ($S^2C^23^2$)

The security dimension forms the important elements for the model such as Integrity, Availability, and Confidentiality, Security Techniques, Provenance, Governance and Accountability.

The model works upon 3 three domains and each Domain contains three processes as shown in figure. These processes are collection of activities and controls to achieve cyber security. Each process take input from one or more sources (including other processes) and produce output (including output to other processes).The processes applies to security technology at various level of security such as operational, physical, Network, Application, and at Database level. All processes are interconnected with each other.

7.3.1 Cyber Security Risk Assessment

The Cyber Security Risk Assessment domain ensures that the various types of risk are identified, analyzed, prioritized and presented in business terms. To support cyber security risk assessment stakeholders make use of tools and techniques and methodologies that are used to asses risk. This risk assessment information is collected, processed and communicated to other processes. The purpose of the risk assessment domain is to identify Threats, Vulnerabilities, Impact (consequences or opportunity) and Likelihood (Probability or frequency an event will occur) and evaluate these against Cyber Cafe business processes.

There are three processes in this domain with different key activities:

- **Capture and Maintain Risk Related Data:** For risk assessment different type of data need to be collected. Existing security policies and procedures are reviewed and documented. Historical threats and vulnerabilities are reviewed along with their impact. Security applied at physical level and technical level is assessed. All the security and network components are assessed. Identify Cyber Cafe security requirements that are important and needs to implement to protect assets. Review should be taken based on implementation and usage of firewall, server logs, internet and network connections, network architecture and Wi-Fi security measures. Authentication mechanism used for authentication and authorization should be reviewed. Also the awareness among the stakeholders for Cyber Cafe security should be studied. Collection of the above data will give output about vulnerabilities, emerging threats and risk factors (frequency, magnitude and impact).
- **Identify, Analyze & Evaluate Risk:**
  For taking the risk decision it is necessary to Identify, Analyze and Evaluate risk. For these assets, threats and vulnerabilities are assessed

along with their impacts and frequency of occurrences. The impact can be found out by finding loss or gain or harm associated with the risk. The external and internal threats both should be considered. Internal threats can be through the operators done purposefully or by mistake such as installing the key logger software or it can be accidental such not changing the router id and password frequently. Based on the data collected evaluate the risk and identify the controls to mitigate the risk. For each control identified its effects should be evaluated. The risk identified should be prioritized and appropriate actions should be considered such as avoid, reduce/mitigate, transfer/share, accept and exploit/seize. For the risk response the cost required and after effects should be identified.

- **Maintain Risk Summary:**

  Summary of data collected from the earlier processes are maintained in a proper format. This information is communicated to stakeholders and can be used for future use. This information will consist of all details such as type of risk, existing controls and procedures, methodology and technology used, controlling authorities, risk type, frequency impact and response considered. This summary register should be updated on regular basis.

7.3.2 Cyber Security Risk Response

Asset is the major things which need to be protected. It may be visitors assets such as visitor’s personal information or information related to his/her web activities and log. Owner’s assets can be system resources, network resources and log details. Assets can be national assets such as government websites, infrastructure, official documents and many more. These assets can be at risk and thus proper risk response management is required.

In the Risk Assessment process the risk are captured and analyzed. These risks are addressed in this process by taking some action. A mitigation plan is made to respond to the risk. Various tools and technologies can be used for responding to risk. Technology along with combination of policy and planning will maximize the protection of Cyber Cafe. Action taken can be accepting the risk, avoiding the risk, sharing the risk or transferring the risk.

There are three processes in this domain with different key activities.

- **Response planning and Assets Security:**

  Data collected in risk assessment processes is used for risk response. Different security tools and techniques at different level of security will help to protect the assets of the stakeholders. Proper authentication and authorization are to implemented. Use of strong password, changing the passwords frequently, and making use of strong password, is necessary. Accessing of resources and modifying them should be prevented. Securing the assets will lead to better Cyber Cafe security.

  Various procedures are identified depending upon the risk by considering the outcome of loss, degree of risk and priority of risk. The time requirement is also considered and before implementing the risk response and possible impact are put forth. Appropriate risk response are selected and approved and disapproved by authorities, and then implemented.

- **Communicate and Manage Risk:**

  The risk responses considered are communicated with all the stakeholders in the process. The information communicated will include the risk considered, its priority, control mechanism, technology and tools considered, earlier similar kind if risk responses if exist, the response effectiveness and response impact if taken. After the risk responses are considered proper documentation is done about risk response that weather it was accepted or not, and what actions were considered. This information is then communicated to other stakeholders for plan preparation.

- **Respond to risk, Incident Handling and Monitor Risk:**

  The risk is responded in this process. Effective measures are considered to for deployment of controls to respond to risk. Before making use of the control reviews about the controls are studied and proper testing is done. The stakeholders are trained for making use of the control and procedures. After implementing the control the risk response is monitored and verified. The outcome is evaluated and corrective actions are taken when needed. Finally the risk response related data are documented with details such as root cause, response taken, environmental and operational requirements and outcomes. These are then communicated to different processes and all stakeholders.

7.3.3 Cyber Security Risk Governance:

This forms the basis for cyber security risk management. It will help the Cyber Cafe business put in place thorough protection. It will help in guiding the use of technology within the business.

Most important requirement for this process is collect information from other processes such as cyber security risk assessment processes and cyber security risk response.

- This process focuses on policies, procedures and processes to manage risk and help to monitor risk which can secure business operations.
- Requirement for cyber security in terms of operational and infrastructure are identified and communicated to stakeholders.
- Policies should be continuously updated as per the rapid growing information environment.

There are three processes in this domain with different key activities.

- **Policy Making and Risk Awareness by Training and Technology usage:**

  In this process Cyber Cafe security policies should be defined. It should provide the documentation processes for risk and risk measurement techniques. Operational policies should be delineated so that risk can be managed. Review should be taken on periodic basis to check the working of operational policies. The gaps and future risk should be identified. Targets based on acceptable risk should be considered with time limits and required resources. Stakeholders should be appropriately trained and made aware about cyber security risk. Their knowledge will help them to take necessary steps for cyber security. During this process the legal requirements are also considered and understood.

- **Audit, Compliance, Review &Support:**

  The policies established for Cyber Cafe security under the law, supports the compliance of various cyber security activities for completing the audit process. The audit is to be done on regular interval for assessing the current implementation of policies and processes. The stakeholders for controlling and assessing the security are identified and allocated the duties. Proper hierarchy needs to be maintained among stakeholders for assigning the roles and responsibilities. The responsible stakeholders has to take review on regular basis and provide support when required along with that the review should be recorded in a proper format and communicated to higher authority as per the policy.

- **Make Business decisions :**

  The stakeholders have to collect information from all the three processes and decide the strategy for business operations. For this proper reporting must be done from all the responsible stakeholders. The risk identified and risk responses considered are considered to take business decision. The business decisions taken are well documented and communicated to all stakeholders. The outcome of business decisions are also documented for future use.

Table No. 7.1 shows the different types of Operational Security Risk, its potential impact and also Risk management for it. Table No.7.2 shows the different types of Physical Security Risk, its potential impact and also Risk management for it and Table No.7.3 shows the different types of Network Security Risk, its potential impact and Risk management for it.

Table No. 7.1: Operational Security Risk

Risk Category	Types Of Operational Security Risk	Potential Impact	Risk Management (Mitigation)
Operational Security Risk	Inadequate Security Training and Lack of Awareness.	Potential of weakness can be exploited. For e.g. Surf porn sites, which often compromise workstations with bots or worms.	Ensure that the security awareness and training is provided to stakeholders at regular interval for which the degree and nature of training may vary. Regular updates and alerts from security websites for security can be checked.
	Insufficient identity validation and background checks.	Identifying the attackers become difficult as the human factor must always be considered the weakest element.	Appropriate procedures to conduct background checks of visitors. Further, prior to being granted access to internet service and resources, proper authentication and authorization mechanisms such as password are required.
	Inadequate Patch Management Process for firmware and software.	Loopholes in software are vulnerabilities that can be used to attack the system.	Automate the mechanism of monitoring and receiving alerts when new security patches become available. Make sure that security patches are applied at least weekly or more often as appropriate.
	Unnecessary system access to server or terminal.	Result into deletion of log information or tampering of information.	Periodically review the access lists for each critical resource or system to ensure that the right set of individuals has authorized access. Establish standards procedures and channels for granting and revoking access to resources or systems.
	Inadequate change or improperly configured system/devices.	Leads to an increased risk of vulnerability.	Ensure that all hardware and software are configured securely. When unclear, seek further clarification from vendors as to secure settings and do not assume that shipped default settings are secure.
	Inadequate periodic security audits.	Leads to unidentified security risk or vulnerability.	Ensure periodic security audits that focus on assessing security controls at the various levels, such as people and policy, operational, network, application, process, and physical security. Security audit provides the status of the implemented security in terms of conformance and policy and determines whether there is a need to

			enhance security policies and procedures.
	Inadequate risk management process.	Leads to inadequate understanding, predicting future risk and poor decision making.	Risk identification and assessment documentation must be done that include vulnerabilities exploitation, risk priority identification, risk response decision, and management of risk.
	Inadequate incident response process.	Response action cannot be taken in timely manner increasing the duration of risk exposure.	Ensure that a proper response process is in place to ensure proper notification, response, and recovery in the event of an incident.

Table No. 7.2: Physical Security Risk

Risk **Category**	**Types Of Physical Security Risk**	**Potential Impact**	**Risk Management (Mitigation)**
Physical Security Risk	Lack of Plan and protection of physical assets	Adversely affect the confidentiality, integrity, and availability of data.	Physical security is an important layer of the overall security strategy and should be applied as appropriate. Protecting physical resources like machines, access point, wires and proper plan for network structure should be there.
	Lack of documentation and monitoring physical access to access point at all times	Tracking of access to access point will be difficult.	Technical and procedural controls for monitoring physical access at all access points at all times must be implemented and documented. Unauthorised access should be detected and appropriate action for unauthorised access should be there.
	Lack of log retention and testing.	Difficulty in tracking of access to resource.	Defined procedure should be there to perform historical analysis of physical access.

Table No. 7.3: Network Security Risk

Risk Category	Types Of Network Security Risk	Potential Impact	Risk Management (Mitigation)
Network Security Risk	Insufficient Log management	Detection of critical events will be difficult and will lead to removal of forensic evidence.	Central Log management should be there for logging events from all devices and alerts should be there in case of problematic events.
	Lack of security mechanism	Lead to unwanted traffic, DoS/DDoS, Session hijacking etc.	Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic moving in network should be there by default.
	Lack of data protection	Modification of data can take place by attacks such as man in middle attacks.	Ensure confidentiality and integrity of that data traversing through network by protecting data through protocols guarantying encryption or apply data level encryption. Biometrics or digital finger print can be used. Timestamps to protect against replay attacks can be used.
	Use of non-standard protocols	Leads to targeting loopholes in protocol and eventually network attacks take place.	Ensure that only standard, approved, and properly reviewed communication protocols which have been examined for security weaknesses are used on the network.
	Inadequate process for network monitoring.	High possibility of anomalous /malicious behaviour via automated and manual techniques.	Detect Intrusion by Intrusion detection system.
	Lack of accountability	Misuse of network may take place.	Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual credentials Enforce accountability.
	Mismatch in accurate timings and node timings.	Historical log maintenance will have improper data and of no use.	Ensure that the source of network time is accurate and that accurate time is reflected on all network nodes for all actions taken and events logged. Maintain accurate network time.
	Lack of unique identification of network resources	Create problems for maintain log without unique identification.	All resources connected to network should be uniquely identified on network. Hardware control should be provided.

Table No. 7.4: Application and Platform Security Risk

Risk Category	Types Of Application and Platform Risk	Potential Impact	Risk Management (Mitigation)
Application and Platform Security Risk	Absence of Malware detection software	Results in infected files and loss of data or may even harm the hardware.	Ensure use of latest and updated Antivirus/Malware software. Software like tripwire can be used to detect infection to file system
	Use of infected devices.	Lead to infection for software and other files.	Ensure that all unneeded services and interfaces (e.g., USB) are turned off on hosts and cannot be ON without permission.
	Unauthorised access	Harm the system and data or may also result in loss of data or tampering of data.	Ensure server passwords and wireless passwords are complex and check for accountability.
	Illegal installation of software's	Create problems of hacking, or removal of log data etc. e.g. Deepfreeze or key loggers are illegal soft wares	Ensure that software installations are not done without permission.

7.4 Risk Response Options and Prioritization with Threat Analysis Parameters

Cyber Cafe is associated different types of risk. Risk is equal to threat, vulnerability and its impact. The stake holders need to monitor threat occurrence and respond to these risks depending upon its analysis. The analysis of risk is done depending upon various factors.

The various factors are –

- Frequency of the threat and type of threat.
- Cost required for response of the risk like in case of mitigation-cost of consulting expert, hardware/software required, implementation cost, monitoring cost, infrastructure cost etc.

  After finalizing the response type it should be found out, how much effectively it can be implemented with existing capabilities or need to look out for new methods or resources. If new technology is implemented its reliability, ease of integration and consequences need to be studied for effectiveness.

- Before implementing the response, pilot study can be done to find out its effectiveness i.e. the extent to which the response will reduce the frequency and impact of the risk.
- Efficiency of the response i.e. the relative benefit by the response.

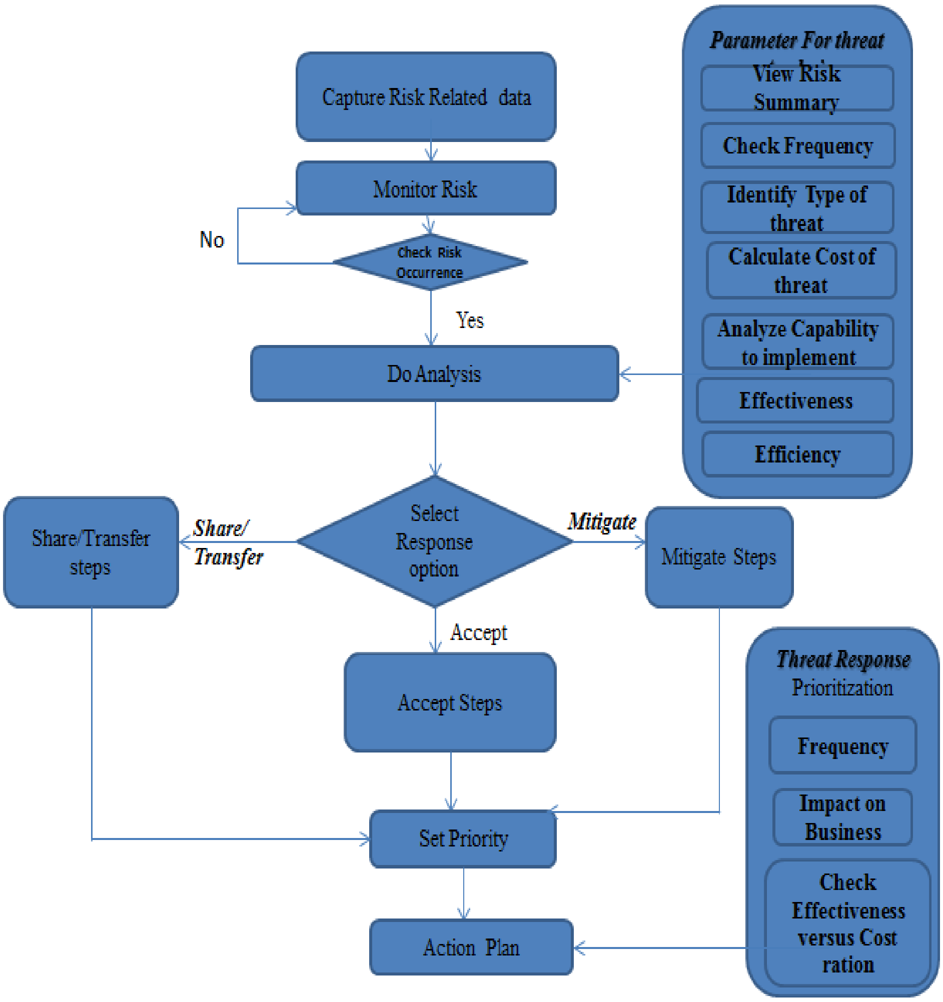


Fig.7.4: Risk Response Options and prioritization with Threat Analysis Parameters

Depending upon these factors various responses such as risk avoidance, risk transfer/risk sharing and risk mitigation can be considered. Risk response option selection is done on the basis of prioritization. The priority will be decided depending upon frequency, its impact on business and its effectiveness versus cost ratio.

Finally Action plan is decided and implemented for effective cyber security.

7.5 Suggestion

For a better tomorrow we need to have a better today and so if we want to secure future from cyber-crime attacks through Cyber Cafe we need to have a better security system for Cyber Cafe today. Consideration of the Owner's problems for cyber security implementation is important along with visitor's problem visiting the Cyber Cafe. The entire cyber security management should be implemented in a way which will protect Cyber-crime from taking place as well as Owners will find it easy to implement cyber security, visitors will be able to visit Cyber Cafe without hesitation and it will be easy for government to ensure that cyber-crime will be avoided because cyber security management at Cyber Cafe is maintained.

Following are some suggestions for the successful implementation of cyber security management system at Cyber Cafe.

- **Awareness programs on cyber security and cyber-crime:** Cyber security begins with a simple message everyone using the Internet can adopt that is to take security and safety precautions, understand the consequences of the actions and behaviors. For this more awareness about cyber security is a must.
    - ➢ Instead of feeling hesitated to use the Cyber Cafe the visitors must be able to use Cyber Cafe for their growth and have social security.

    - The government should also arrange, encourage and subsidize IT vocational training or compulsory subject to create an IT-literate society with an awareness of cyber security.
    - Awareness can also be done by using traditional methods using media vis. namely radio, television, newspaper etc.
    - Need to create awareness of Wi-Fi internet services among Owners.
    - Awareness programs about cyber security can also be arranged by corporate sector or NGO for general citizens to prevent cyber-crime.
- **Training programs for Cyber Cafe Owners:** Lack of proper cyber security training for owners could create security breaches in Cyber Cafe. It may happen that Owner of the Cyber Cafe network does not know how breaches could occur and may not be aware of how to avert such insecurity.
    - Security awareness and training should be made part of the rules and regulations of Cyber Cafe.
    - For this purpose it should be mandatory for all Owners to undergo a cyber-security management training which should be provided by the government and Cyber Cafe license should be issued only after completion of training.
    - Government should issue Cyber Cafe license only to those Owners who has completed cyber security training course under government.
- **Mandatory login for government cyber security websites or security organization Government:**
    - The Cyber Cafe Owners should have account with government websites which take care about cyber security or problems related to it and they should visit and login regularly.
    - Due to this they can come to know about current cyber security loopholes if any and understand how to take necessary precautions.
    - The websites such as computer emergency response team (CERT) which is regarded as perhaps the Internet-best known security

organization. Due to this initiative the Owners will be benefitted and there can be a transparent communication between the government cyber security expert and the Owners.

    - The government can also get a common platform to share cyber security related information with the Cyber Cafe Owners using video conferencing.

- **Manage and update cyber security content on government websites efficiently and regularly**:
    - The government should take effort to manage and update the cyber security website on regular basis.
    - Updates should be done by security experts. Also regular updates related to Cyber Cafe rules and regulations should be reflected and confirmed that each Cyber Cafe Owners reads it along with cyber security details.
- **Efforts on the line of localization**:
    - It will create a great impact if cyber security updates and awareness are made available in the local languages. This will be helpful not only to Cyber Cafe Owners but also to visitors to know about cyber security and to take necessary precautions to avoid cyber-crime.
    - Translation conversion measures should be given keeping in mind the visitors may not be computer savvy or highly literate.
- **Security software**
    - Common for all Cyber Cafes which can take care about cyber security and day to day business transaction can be created. This software will connect to government software and should be regularly updated.

- **Amendments in the rules and regulations for Cyber Cafe put forth by the government:**
  - Government Rules and regulation governing the internet and Cyber Cafe should be amended on regular basis and intervals since things on internet changes at a faster rate along with emergences of many cyber threats.
  - There should be improvement in the development of the network security to reduce the number of online attacks and amend the rules and regulations. Better security standards are necessary.
- **Suggestion related to some changes in existing Cyber Cafe laws:**
  - Instead of taking photograph for which many visitors have objection biometric system can be used as suggested in the model or UID can be used and log can be uploaded on government accessible cloud.
  - For children in case not accompanied by adult should be provided a special computer zone where parental settings or proper privacy settings are already been done. This will help children's from poor class to access internet where security will be already provided.
  - Instead of compulsory log registers maintenance for 2 years a common storage space and common software for all Cyber Cafe's which will be controlled and connected by the government can be implemented which will store the log details for Cyber Cafe on the cloud and whenever required can be accessed by the government.
  - In another rule it is given that "The cyber café Owner shall be responsible for storing and maintaining following backups of logs and computer resource records for at least six months for

each access or login by any user. Instead for period of six months such details can be placed on the cloud in the space provided by the Cyber Cafe.

It is easier for cyber-crimes to take place as per the architecture suggested by law, identity theft can take place since it would be easier to observe the login details of other users at the Cyber Cafe.

  - Instead of the rule that an officer not below the rank of Police Inspector will check or inspect Cyber Cafe, it is suggested that the web camera which is already a mandatory part as per law can be connected to the common software between Cyber Cafe and the police authorities. This will stop the unregulated and unsupervised powers by any government official. Thus it will reduce the burden of owners. Already the provision of Shops and Establishments Acts of most states already prescribe a procedure for inspection. A surprise visit once in a year can be done by authorities and can be recorded.

- **Security suggestions for Owners:**
  - Owners need to take efforts for effective implementation of cyber security management at all levels of security in Cyber Cafe so that their business can be improved.
  - At physical level protection of assets must be done. The server room should be separate preferably closed rooms. The cables should be protected from external damage. Position the router or access point at a suitable and safer location and not nearby window or door. Power fluctuations or drops in voltage may cause loss of data or fall victim to disk crashes or hardware damage. A variety of hardware techniques can be used such as voltage regulators, noise filter ,grounding techniques, can be used to combat these problems
  - At operational level Owners must ensure securing the Cyber Cafe both internally and externally by following a proper defense

mechanism consisting of boarder security (against external and internal attackers).Internal threats can occur in case operator is hired to look after Cyber Cafe activities and that person is criminal minded. Such person may hamper the security in many ways such as installing illegal software like key logger software. Internal threats can also occur due to operator incompetence. So care must be taken while employing any person in the cafe.

- At Software level security steps such as updating the operating system or application software, antivirus installation and up gradations, virus scanning etc. should be done on regular basis.
- At database level the logs maintained on the server or cloud should be protected. Access to server or data stored place should be restricted from unauthorized visitors. Back up should be taken at regular interval and placed at a secured place. Whenever any illegal attempt is made to gain an access to the system there should be a mechanism or process which will proactively test vulnerabilities on regular basis and take proper action wherever required.
- At network level fire walls, intrusion detection, virtual private networking, denial-of-service protection, authentication such as biometrics etc. should be done on regular basis. In case of Wi-Fi network disable SSID broadcast, avoid connecting to open Wi-Fi networks, assign static IP addresses to devices, Enable firewalls on each computer and router, and turn off the network when not in use.
- Owners should cooperate with law authorities and law enforcement agencies for proper cyber security management and to help prevent against them being compromised or used against others.
- Owners should display the cyber security assistance in terms of display boards in the cafe for help to the visitors.

- **Security suggestions for Visitors:**
  - Visitors should make themselves aware about cyber security and cyber-crime. If technology is to be used the advantages and disadvantages should also be studied before using it.
  - It is always said that prevention is better than cure. Thus if proper security precautions are taken cyber-attacks can be avoided. While using Cyber Cafe following care should be taken by visitors.
    - Password Management – different password for different websites, changing password at regular interval especially after visit to public internet access change of password is a must. Along with this strong passwords must be set having alphanumeric pattern.

    - Personal Information Sharing: It is advised that personal information should be avoided and never telling the password to unknown person. Keep an eye on stranger especially in public internet access places who may try to access the information. Never to leave the computer unattended in Cyber Cafe and always being alert if people viewing the screen. Having a separate email accounts for official work and private work. Social Networking websites are useful but care should be taken while sharing personal information on it as it becomes public once it is uploaded. Proper security options provided by websites should be used.

    - Use of Technology for security: Whenever accessing internet through public places like Cyber Cafe make use of private browsing which will not allow any browser to store browsing history cookies, search history, download history, web form history, and temporary internet files. Making use of secure web link and not clicking on unknown links. Disable all file sharing. Check for updated antivirus and AntiSpyWare/malware software installed. Not to open email attachment from unknown links. Also make use of updated and license software including operating system. Where ever possible disable Java, JavaScript, and ActiveX. Always log out from all accounts whenever leaving the Cyber Cafe.

7.6 Scope for Future Research:

Cyber Security is a broad field. Lots of work can be studied in the future. Over time, the variety and sophistication of network attacks are likely to increase. Thus there is requirement for ongoing research in this field that can cater for the new challenges. Since in depth studies in these areas have long term social-economic dimension and repercussions, the scope of the investigation can be further expanded as follows:

- ➢ Since it was observed that less number of registered Cyber Cafe have Wi-Fi services provided, the researcher has not considered in depth study of cyber security for Wi-Fi, which is bound to grow in most of the cafe. Further research can be done related to Wi-Fi services in public areas.
- ➢ Due to limitation of time in obtaining data from Cyber Cafe the work has been restricted to geographical areas of Pune city. Rural area can be considered for further research which can be more useful, informative and illuminating.
- ➢ Researcher has studied Cyber Cafe Owners and visitor’s perspective and problems related to cyber security. Further research can be taken to study government officials and police authorities’ perspective and problems related to cyber security implementation.
- ➢ The researcher has considered Cyber Cafe problems related to security, further study related to other public places where internet

services are provided such as Hotels, Restaurants, and Airports etc. can be considered.

- Further research can also be focused on the role of Cyber Cafe management software in controlling and eradicating Cyber-crimes.

Annexure 1

Questionnaire for Cyber Cafe Owner

Dear Sir/ Madam,

As you are aware, the Owner of Cyber Cafe is experiencing no of problems related to cyber security. Government has made new policies, rules and regulations to prevent Cyber-crime through Cyber Cafe. The researcher is studying cyber security management system aspect of cyber café as a part of doctoral research work and is interested in survey of cyber café in Pune city. We will keep confidentiality of your data. Data will be exclusively used for academic research work.

Details of Cyber café

1) Cyber Cafe Name - ________________________________

2) Cyber Café Location/Road Name :______________________________

3) Area under police station(Tick the appropriate box):

Area under police Station			
1. Faraskhana □	2. Lashkar □	3. Chatturshrungi □	4. Khadki □
5. Khadak □	6. Bund garden □	7. Hinjewadi □	8. Vishrantwadi □
9. Vishrambaug □	10. Samarth □	11. Sangvi □	12. Yerwada □
13. Shivajinagar □	14. Swargate □	15. Pimpri □	16. Vimantal □
17. Deccan □	18. Dattawadi □	19. Bhosari □	20. Wanwadi □
21. Kothrud □	22. Sahakarnagar □	23. Nigdi □	24. Hadapsar □
25. Warje Malwadi □	26. Bharati Vidyapeeth □	27. Chinchwad □	28. Kondhwa □
	29. Koregaon Park □	30. Mundhwa □	31. Marketyard □

4) Ward Office Name (Tick the appropriate box):

1. Aundh □	2. Kothrud/Karve Rd □	3. Ghole road □	4. Warje Karve Ngr □
5. Yerwada □	6. Bibwewadi □	7. Bhavani peth □	8. Dhankwadi □
9. Sahakarnagar □	10. Hadapsar □	11. Sangamwadi/ Nagar Road □	12. Kasba □ VishramBagwada
13. Dhole Patil □	14. Tilak Road □		

5) Have you registered your Cyber Cafe?

Yes □ No □

6) Do you have your website for Cyber Cafe?

Yes □ No □

7) Number of Computers in Cyber Cafe: (Tick the appropriate box)

i. 0 - 5 □	ii. 6 – 10 □	iii. 11 - 15 □	iv. 16 – 20 □	v. 21 – 25 □

8) Approximate set up cost invested for cyber café (Tick the appropriate box) –

i. Cost of Software

a) 1 up to 20 thousand □	b) 21 thousand to 40 thousand □	c) 41 thousand to 60 thousand □	d) 61 thousand to 80 thousand □	e) Above 80 thousand □

ii. Cost of hardware

a)Up to 50 thousand □	b) 51 thousand to 1 lacs □	c)1 lacs to 1.5 lacs □	d)1.5 lacs to 2 lacs □	e)Above 2 lacs □

iii. Cost of Other Infrastructure

a)Up to 20 thousand □	b) 21 thousand to 40 thousand □	c) 41 thousand to 60 thousand □	d)61 thousand to 80 thousand □	e)Above 80 thousand □

iv Total Cost - ______________________________

Details Of Cyber Owner

9) Qualification(Tick the appropriate boxes) :

1. Up to Higher Secondary □	2. Higher Secondary and above □
3. Up to Graduation □	4. Post graduation & above □

10) Do you have any background in Computer Technology? (Tick the appropriate box)

Computer Back ground	**Yes**	**No**
Short Term Course in computers	□	□
Computer Diploma	□	□
Computer Degree	□	□
Professional Certification	□	□

Details of Cyber Café Business

11) What type of internet service connection type do you provide? (Tick the appropriate boxes)

Connection Type	**Yes**	**No**
1. Dial up Connection	□	□
2. Broad Band	□	□
3. Broad Band Wi-Fi	□	□

12) Which internet service provider do you have? (Tick the appropriate boxes)

1. Airtel □	2. Tikona □	3. BSNL □	4. Airmesh □
5. Tata DOCOMO□	6. Hathway □	7. MTS □	8. Powernet □
9. Idea □	10. Aircel □	11. O-Zone □	12. Reliance □ Communication
13. Delight □	14. Wi-5 □	15. Spectranet □	16. Tata Indicom □
17. D-Vois □	18. Sify □	19. Vodaphone □	20. TATA(VSNL) □

13) What are the average charges per hour? (Tick the appropriate box)

1. Less than Rs.15 □	2. Rs.15-less than Rs.20 □	3. Rs.20 – less than Rs.25□	4. Rs.25- less than Rs.30□	5. Rs.30-more than Rs.30□

14) Do you provide member ship facility for cyber café users? (Tick the appropriate box)

Yes □ No □

If Yes

i. What is the duration of membership? (Tick the appropriate box)

a)Up to 15 days □	c) 16 days – 1 months □	c) more than 1 months to 1.5 months □	d) more than 1.5 months to 2 months □	e) Any other ______________

ii. What are the average member ship charges? (Tick the appropriate box)

1. Up to Rs.100 □	2. Rs.101 to Rs.150 □	3. Rs.151 to Rs.200 □	4. Rs.201 to Rs.300 □	5. Above Rs.300 □

15) On an average what are the number of visitors visiting the Cyber Cafe in a day?

(Tick the appropriate box)

1. Up to 20 □	2. 21 to 40 □	3. 41 to 60 □	4. 60 to 80 □	5. Above 80 □

16) What are your monthly expenses for running the cyber café? (Tick the appropriate box)

1. Up to Rs.10000 □	2. Rs.10001 to Rs.20000 □	3. Rs.20001 to Rs.30000 □
4. Rs.30001 to Rs.40000 □	5. Rs.40001 to Rs.50000 □	

17) Along with Internet service do you provide any other kind of service to cyber café users?

(Tick the appropriate boxes)

Services	**Yes**	**No**
1. Printing	□	□
2. Lamination	□	□
3. Mobile Recharging	□	□
4. Software Creation	□	□
5. Photo Copying	□	□
6. Computer Product	□	□
7. Creation of letter head	□	□
8. Scanning	□	□
9. CD Writing	□	□
10. Creation of resume	□	□

11. Fax Machine	□	□
12. Gift and Stationary	□	□
13. PDF Conversion	□	□
14. Play station(or Game)	□	□
15. Computer Training	□	□

18) What policy do you have to maintain cyber café? (Tick the appropriate boxes)

Maintenance Policy	**Yes**	**No**
1. Self	□	□
2. Using Software	□	□
3. Using Cyber Cafe Website	□	□
4. Remotely through third party	□	□

19) Rate the following problems factors faced while running Cyber Cafe business

Strongly Agree(SA)-5,Agree(A)-4,Neutral(N)-3,Disagree(D)-2,Strongly Disagree(SD)-1

Factors	**SA(5)**	**A(4)**	**N(3)**	**D(2)**	**SD(1)**
1. Lack of established resources to know about cyber security updates.	□	□	□	□	□
2. Lack of knowledge about cyber security maintenance.	□	□	□	□	□
3. Lack of resources to assist in case of Cyber-crime attack.	□	□	□	□	□
4. Lack of established indicators that would indicate an attack is underway.	□	□	□	□	□
5. Reputation hampered due to Cyber-crimes	□	□	□	□	□
6. Cost of maintaining Cyber Cafe is high	□	□	□	□	□
7. Stealing of hotspot account and payment information (Wi-Fi)	□	□	□	□	□
8. Slow Down of network (Wi-Fi)	□	□	□	□	□
9. Login information to unsecured sites and content(Wi-Fi)	□	□	□	□	□
10. Data Integrity attack(alteration of data) (Wi-Fi)	□	□	□	□	□
11. Advertising Private key (Wi-Fi)	□	□	□	□	□

20) Do you have Licensed software in your cyber café? (Tick the appropriate box)

Yes □ No □

21) Do you use Software for cyber café execution:

Yes □ No □

If Yes Name the Software:___________________________

About Cyber security in Cyber Cafe

22) How do you maintain cyber security? (Tick the appropriate box)

Cyber Security Maintenance Method	**Yes**	**No**
1. Self	□	□
2. Using Automated Software	□	□

23) At what level are you maintaining the cyber security? (Tick the appropriate boxes)

a. End point □	b. Gate Way Level □	c. At Both Level □

24) What techniques are you aware and implement for cyber security? (Tick the appropriate boxes)

Security Techniques Aware and Implemented	**Aware**		**Implement**	
	Yes	**No**	**Yes**	**No**
1. Antivirus	□	□	□	□
2. Endpoint security s/w	□	□	□	□
3. Antispyware software	□	□	□	□
4. Firewall	□	□	□	□
5. Network Access Control	□	□	□	□
6. Control Panel access restriction	□	□	□	□
7. Browser Security options access restriction	□	□	□	□
8. Physical drive access restriction	□	□	□	□
9. Security option access restriction	□	□	□	□
10. Changing routers administrator username and password	□	□	□	□
11. Blocking Installation and setup files	□	□	□	□
12. Remote Client Monitoring	□	□	□	□

13. UTM (Unified Threat Management)	□	□	□	□
14. Website or keyword blocking	□	□	□	□
15. Content Filter	□	□	□	□
16. Browser Security	□	□	□	□
17. Manually turn off Wireless Router /Access Point(Wi-Fi)	□	□	□	□
18. Change the default username and Password of the Access Point(Wi-Fi)	□	□	□	□
19. Disabling Auto Connect Mode(Wi-Fi)	□	□	□	□
20. Disabling SSID broadcasting (Not broadcasting network name) (Wi-Fi)	□	□	□	□
21. Shutdown the Access Point when not in use(Wi-Fi)	□	□	□	□
22. Placing Wireless Router/Access Point inside building(Wi-Fi)	□	□	□	□
23. Disable DHCP service when less users (Wi-Fi)	□	□	□	□
24. WPA(Wi-Fi Protected Access) (Wi-Fi)	□	□	□	□
25. TKIP(Wi-Fi)	□	□	□	□
26. WEP(Wired Equivalent Privacy) (Wi-Fi)	□	□	□	□
27. IEEE 802.11i(WPA2) (Wi-Fi)	□	□	□	□
28. Storing MAC address(Wi-Fi)	□	□	□	□
29. Filtering MAC address (Wi-Fi)	□	□	□	□
30. Filtering IP address (Wi-Fi)	□	□	□	□
31. Block anonymous IP address(Wi-Fi)	□	□	□	□

25) What type of Physical security do you provide? (Tick the appropriate boxes):

Physical Security Type	**Yes**	**No**
1. Locking of PC cases	□	□
2. Break Glass alarm sensors	□	□
3. All external opening windows to have locks	□	□
4. Detectors	□	□

5. Intruders alarm sensor on access router	□	□
6. Separate server inaccessible to users	□	□

About awareness of existing controls, processes & policies for Cyber Cafes

26) For prevention of Cyber-crime do you have any provision in terms of: (Tick the appropriate boxes)

Cyber Crime Prevention Provision	**Yes**	**No**
1. Displaying Poster for not accessing restricted websites by government	□	□
2. Rules for accessing Cyber Cafe	□	□
3. Displaying Government Rules for cyber café.	□	□

27) Do you maintain Following things and for what duration? (Tick the appropriate boxes):

Cyber Cafe Things Maintained	**Aware**	**Not Maintained**	**Maintained**				
			Durations of Maintenance				
			Up to 6 months	**Up to 1 year**	**Up to 1.5 year**	**Up to 2 year**	**Above 2 year**
1. Log register for users	□	□	□	□	□	□	□
2. Backup of Log registers	□	□	□	□	□	□	□
3. Web Camera	□	□	□	□	□	□	□
4. Back up of Web Camera	□	□	□	□	□	□	□
5. Computer Access records	□	□	□	□	□	□	□

28) Do you have Fire Extinguisher?

Yes □ No □

29) Which type of records do you maintain?(Tick the appropriate boxes)

Type Of Record Maintained	**Yes**	**No**
1. History of websites accessed using computer resource at Cyber Cafe	□	□
2. Logs of proxy server installed at cyber café	□	□
3. Mail server logs	□	□

4. Logs of network devices such as router, switches, systems etc. installed at cyber café	□	□
5. Logs of firewall or Intrusion Prevention/Detection systems, if installed	□	□

30) What documents do you check for identification purpose? (Tick the appropriate boxes):

Documents	**Yes**	**No**
1. Student Educational ID	□	□
2. Photo Credit Card	□	□
3. UID /PAN card	□	□
4. Voters Card	□	□
5. Employee ID Card	□	□
6. Photo Debit Card	□	□
7. Driving License	□	□

31) What type of cubicles do you provide? (Tick the appropriate box)

1. Open cubicles □ 2. Closed Cubicles □

32) If open cubicle, what is the size of cubicle that you provide?

1. 1.5 Feet □	**2.** 2.5 Feet□	**3.** 3.5 Feet□	**4.** 4.5 Feet□	**5.** More than4.5 Feet

33) Do you install any software which cleans data of user after use so that no crime occurs?

Yes □ No □

a)If Yes, specify the name of software:________________________________

34) What is your view about Cyber Cafe regulation? (Tick the appropriate box)

Cyber Cafe regulation's owners view	**Yes**	**No**
1. There is huge decline in number of Cyber Cafe Visitors**.**	□	□
2. There is increase in Cyber-crime awareness	□	□

35)

In your Cyber Cafe(Tick the appropriate box)	**Yes**	**No**
1. Do all open machines face outward, i.e., facing the common open space of the Cyber Café?	□	□
2. Do you use shared Internet protocol address for client machine?	□	□
3. Do you maintain an electronic log that shows the mapping of a unique physical Internet Protocol with the 'masqueraded' Internet Protocol address?	□	□
4. Do you maintain a list showing which Internet Protocol Address is allocated to which machine?	□	□
5. Are you aware about Indian Computer Emergency Response Team?	□	□
6. Do you refer to Guidelines for auditing and logging – 'CISG – 2008-01'for assistance related?	□	□

36) Which type of Cyber-crime you are aware about? (Tick the appropriate boxes)

Cyber Crime Type	**Yes**	**No**
1. Cyber pornography	□	□
2. Intellectual Property Crimes	□	□
3. Money Laundering and Evasion	□	□
4. Electronic Funds Transfer Fraud	□	□
5. Hacking	□	□
6. Email Spoofing	□	□
7. Political Crime	□	□
8. Electronic Terrorism	□	□
9. E-Murder	□	□

37) What is the nature of complaint registration that you are aware of? (Tick the appropriate boxes)

Complaint Registration Nature(Method)	**Yes**	**No**
1. Internet	□	□
2. Telephone	□	□
3. Personally visiting Cyber-crime Cell or Police Station	□	□

38) In case a Cyber-crime incident occurs where do you register complaint? (Tick the appropriate boxes)

Complaint Registration Place	**Yes**	**No**
1. Cyber-crime Cell	□	□
2. Police Station	□	□
3. Private Detective	□	□
4. Loknyayalaya- Alternative Dispute Resolution System	□	□

39) What is the grade of person coming for cyber café inspection and frequency of visit in a month?

(Tick the appropriate boxes)

Grade		**Visit Frequency**				
	0 times	**1-2 times**	**3-4 times**	**5-6 times**	**6-7 times**	**More than 7 Months**
Police Inspector	□	□	□	□	□	□
Constable	□	□	□	□	□	□
Police sub Inspector	□	□	□	□	□	□
Havaldar	□	□	□	□	□	□
	Any other Specify:______________________________					

40) Is audit done for the Cyber Cafe by the police?Yes □ No □

a) If Yes, What type of security auditing is done?

Security Audit	Yes	No
Manual and Online Register version of Log Register	□	□
Server Log(Proxy server),Event Log	□	□
Network Audit	□	□
Application Security Audit	□	□

41) To what extent are you satisfied with the following? (Tick the appropriate box)

Highly Satisfied(HS)-5,Satisfied(S)-4,Neutral(N)-3,Dissatisfied(DS)-2,Highly Dissatisfied(HD)-1

Satisfaction Criteria	**HS(5)**	**S(4)**	**N(3)**	**DS(2)**	**HD(1)**
1. Audit Done	□	□	□	□	□
2. Inspection Process	□	□	□	□	□
3. Government Rules and Regulations	□	□	□	□	□
4. Government Updates	□	□	□	□	□

42) What is the nature of receiving the updates? (Tick the appropriate boxes)

Nature Of Updates	**Yes**	**No**
1. Government (Police)Website	□	□
2. Personally through Police Inspector	□	□
3. News Paper	□	□
4. Telephone	□	□

Please write Your Suggestions or Recommendations or comments

Thank you for sparing your valuable time and providing information.

Annexure 2

Questionnaire for Cyber cafe Visitors

Dear Sir/ Madam,

As you are aware, Cyber cafe Industry is experiencing many problems related to cyber security issue. Government has made new policies, rules and regulations to prevent cyber crime through cyber cafe. The researcher is studying cyber security management system aspect of cyber café as a part of doctoral research work and is interested in survey of cyber café in Pune city. Your most precise and valuable answers would help us to achieve our Research objectives. We keep confidentiality of your data. Data will be exclusively used for research work.

Details about the cyber cafe

1) How often do you visit cyber café? (Tick the appropriate box):

i. Daily □	ii. Weekly □	iii. Monthly □	iv. Yearly□	v. Randomly □

2) What type of internet service connectivity do you use? (Tick the appropriate boxes)

i. Dialup connection □	ii. Broadband □	iii. Wi-Fi □

3) What are the fees per hour for the cyber café you visit? (Tick the appropriate boxes):

i)Rs.10 □	ii)Rs.20 □	iii)Rs.15 □	iv)Rs.25 □	v)More than Rs.25 □

4) In your view what are the probable reasons for use of a cyber café?
(Tick the appropriate boxes)

Probable Reasons	Yes	No
i. Speed of internet	□	□
ii. Cost benefit for downloading	□	□
iii. Help/Assistance	□	□
iv. Latest Software	□	□
v. Update Software	□	□
vi. Overall comfort level	□	□
vii. Price	□	□

5) What are the activities that you generally do using a cyber café?
(Tick the appropriate boxes)

Activities		Yes	No
i.	Email	□	□
ii.	Social Networking	□	□
iii.	Learning New Things	□	□
iv.	Shopping	□	□
v.	E-governance Services	□	□
vi.	Chatting	□	□
vii.	Playing Games	□	□
viii.	Downloading	□	□
ix.	Net Banking	□	□
x.	Online Buying	□	□
xi.	Printing	□	□
xii.	CD Writing/DVD Writing/Data copy or storage	□	□
xiii.	Software Coaching	□	□
xiv.	Scanning	□	□
xv.	Lamination	□	□
xvi.	Software usage	□	□

6) Which method do you follow to fill the log register kept in cyber café?
(Tick the appropriate boxes):

Method		Yes	No
i.	Manually Filling Register	□	□
ii.	Through Software	□	□

7) Which of the following documents are checked for identification purpose in cyber cafe?
(Tick the appropriate boxes):

Document		Yes	No
i.	Pan Card	□	□
ii.	Voters Card	□	□
iii.	Student Educational Id	□	□
iv.	Employees ID Card	□	□
v.	Photo Credit Card	□	□
vi.	UID	□	□
vii.	Driving License	□	□

8) Which of the following hesitation occur whenever you visit cyber cafe?
(Tick the appropriate boxes):
Strongly Agree(SA)-5,Agree(A)-4,Neutral(N)-3,Disagree(D)-2,Strongly Disagree(SD)-1

Hesitation Reasons		SA(5)	A(4)	N(3)	D(2)	SD(1)
i.	Personal Identification Checking	□	□	□	□	□
ii.	Misuse of personal data	□	□	□	□	□
iii.	Storing website history by owners	□	□	□	□	□
iv.	Increase in cyber crime	□	□	□	□	□
v.	Low Cyber Security	□	□	□	□	□
vi.	Blockage of websites by government	□	□	□	□	□
vii.	Privacy Disturbed	□	□	□	□	□
viii.	Data Loss	□	□	□	□	□
ix.	H/W Devices corrupted due to malicious S/W	□	□	□	□	□
x.	Web Camera	□	□	□	□	□

9) Are you aware about cyber security and what kind of security precautions do you take?
(Tick the appropriate boxes):
Strongly Agree(SA)-5,Agree(A)-4,Neutral(N)-3,Disagree(D)-2,Strongly Disagree(SD)-1

Security Precaution		Aware	SA(5)	A(4)	N(3)	D(2)	SD(1)
i.	Aware about cyber security.	□	□	□	□	□	□
ii.	Not using same password for multiple sites.	□	□	□	□	□	□
iii.	Setting Strong Passwords.	□	□	□	□	□	□
iv.	Checking browsers Privacy Settings.	□	□	□	□	□	□
v.	Separate email account for business and personal use.	□	□	□	□	□	□
vi.	Don’t click on unknown links.	□	□	□	□	□	□
vii.	Connect only with people you know.	□	□	□	□	□	□
viii.	Not sharing personal information with strangers.	□	□	□	□	□	□
ix.	Make use of secure web link.	□	□	□	□	□	□
x.	Changing passwords after visiting cyber café.	□	□	□	□	□	□
xi.	Avoid Financial Transactions.	□	□	□	□	□	□
xii.	Always alert if people viewing the screen.	□	□	□	□	□	□
xiii.	Not to leave computer unattended.	□	□	□	□	□	□
xiv.	Make use of private browsing.	□	□	□	□	□	□

xv.	Checking Firewall is ON.	□	□	□	□	□	□
xvi.	Disable all File Sharing.	□	□	□	□	□	□
xvii.	Machines has latest patches & updates for S/W.	□	□	□	□	□	□
xviii.	Use of antivirus & antispyware/malware programs.	□	□	□	□	□	□
xix.	Using infrastructure Network only and not using adhoc mode & Checking encryption security(Wi-Fi)	□	□	□	□	□	□
xx.	Use Only Encrypted Websites	□	□	□	□	□	□
xxi.	Turn On personal Firewall	□	□	□	□	□	□
xxii.	Turn OFF file sharing	□	□	□	□	□	□

10) Do you read & follow instructions related to cyber crime in cyber cafe?

Yes □ No □

11) Are you aware about cyber crime?

Yes □ No □

If Yes (Tick the appropriate boxes):

Strongly Agree(SA)-5,Agree(A)-4,Neutral(N)-3,Disagree(D)-2,Strongly Disagree(SD)-1

Cyber Crime Awareness		**SA(5)**	**A(4)**	**N(3)**	**D(2)**	**SD(1)**
i.	Phishing.	□	□	□	□	□
ii.	Cyber stalking.	□	□	□	□	□
iii.	Hacking.	□	□	□	□	□
iv.	Pornography.	□	□	□	□	□
v.	Credit card fraud.	□	□	□	□	□
vi.	Email Spoofing.	□	□	□	□	□
vii.	Intellectual Property Crimes.	□	□	□	□	□
viii.	Internet Time Theft.	□	□	□	□	□

12) Which type of cyber complaint registration are you aware of?(Tick the appropriate boxes):

Nature of Cyber complaint registration		**Yes**	**No**
i.	Internet.	□	□
ii.	Cyber crime Cell Police Station.	□	□
iii.	Telephone.	□	□
iv.	No such system.	□	□

13) In case a cyber crime incident occurs where do you lodge complaint?

(Tick the appropriate boxes):

Strongly Agree(SA)-5,Agree(A)-4,Neutral(N)-3,Disagree(D)-2,Strongly Disagree(SD)-1

Complaint Registration Place	**SA(5)**	**A(4)**	**N(3)**	**D(2)**	**SD(1)**

i.	Cyber Crime Cell.	□	□	□	□	□
ii.	Police Station.	□	□	□	□	□
iii.	Private Detective.	□	□	□	□	□
iv.	Loknyayalaya-Alternative Dispute Resolution System.	□	□	□	□	□

14) What type of punishment do you think should be given in case of cyber crime? (Tick the appropriate boxes):

Punishment Type		**Yes**	**No**
i.	Imprisonment.	□	□
ii.	Penalty.	□	□
iii.	Death Sentences.	□	□

15) Gender –Male □ Female □

16) Age in years-

i. 5 -15 □	ii. 16 -25 □	iii. 26 – 35 □	iv. 36 - 45 □	v. Above 45 □

17) Please write your comments or suggestions about Cyber Security and crimes?

____

____

Thank you for sparing your valuable time and providing information.

Annexure - 3

Department Of Information Technology National Cyber Security Policy

"For secure computing environment and adequate trust & confidence in electronic transactions"

National Cyber Security Policy, draft v1.0, 26 Mar 2011

Stakeholder Agencies

1	National Information Board (NIB)
2	National Crisis Management Committee (NCMC)
3	National Security Council Secretariat (NSCS)
4	Ministry of Home affairs
5	Ministry of Defence
6	Department of Information Technology (DIT)
7	Department of Telecommunications (DoT)
8	National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In)
9	National Information Infrastructure Protection Centre (NIIPC)
10	National Disaster Management of Authority (NDMA)
11	Standardisation, Testing and Quality Certification (STQC) Directorate
12	Sectoral CERTs

Department Of Information Technology National Cyber Security Policy “For secure computing environment and adequate trust & confidence in electronic transactions” National Cyber Security Policy, draft v1.0, 26 Mar 2011 18

1 National Information Board (NIB)

National Information Board is an apex agency with representatives from relevant Departments and agencies that form part of the critical minimum information infrastructure in the country. NIB is entrusted with the responsibility of enunciating the national policy on information security and coordination on all aspects of information security governance in the country. NIB is headed by the National Security Advisor.

2 National Crisis Management Committee (NCMC)

The National Crisis Management Committee (NCMC) is an apex body of Government of India for dealing with major crisis incidents that have serious or national ramifications. It will also deal with national crisis arising out of focused cyber attacks. NCMC is headed by the Cabinet Secretary and comprises of Secretary level officials of Govt. of India. When a situation is being handled by the NCMC it will give directions to the Crisis Management Group of the Central Administrative Ministry/Department as deemed necessary.

3 National Security Council Secretariat (NSCS)

National Security Council Secretariat (NSCS) is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB.

4 Ministry of Home Affairs (MHA)

Ministry of Home Affairs issues security guidelines from time to time to secure physical infrastructure. The respective Central Administrative Ministries/Departments and critical sector organizations are required to implement these guidelines for beefing up/strengthening the security measures of their infrastructure. MHA sensitizes the administrative departments and organizations about vulnerabilities and also assists the respective administrative Ministry/Departments.

5 Ministry of Defence

Ministry of Defence is the nodal agency for cyber security incident response with respect to Defence sector. MoD, IDS (DIARA), formed under the aegis of Headquarters, Integrated Defence Staff, is the nodal tri-Services agency at the national level to effectively deal with all aspects of Information Assurance and operations. It has also formed the Defence CERT where primary function is to coordinate the activities of services/MoD CERTs. It works in close association with CERT-In to ensure perpetual availability of Defence networks.

6 Department of Information Technology (DIT)

Department of Information Technology (DIT) is under the Ministry of Communications and Information Technology, Government of India. DIT strives to make India a global leading player in Information Technology and at the same time take the benefits of Information Technology to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion & policies in electronics & IT. Department Of Information Technology National Cyber Security Policy “For secure computing environment and adequate trust & confidence in electronic transactions ” National Cyber Security Policy, draft v1.0, 26 Mar 2011 19

7 Department of Telecommunications (DoT)

Department of Telecommunications (DoT) under the Ministry of Communications and Information Technology, Government of India, is responsible to coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In and other government agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers are able to track the critical optical fiber networks for uninterrupted availability and have arrangements of alternate routing in case of physical attacks on these networks.

8 National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In)

CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organizations in the country. It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs, all over the world; and Sectoral CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the country. It would work with Government, Public & Private Sectors and Users in the country and monitors cyber incidents on continuing basis through out the extent of incident to analyse and disseminate information and guidelines as necessary. The primary constituency of CERT-In would be organizations under public and private sector domain.

9 National Information Infrastructure Protection Centre (NIIPC)

NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies’ ability to collect, analyze and disseminate intelligence. NIIPC would interact with other incident response organizations including CERT-In, enabling such organizations to leverage the Intelligence agencies’ analytical capabilities for providing advanced information of potential threats.

10 National Disaster Management of Authority (NDMA)

The National Disaster Management Authority (NDMA) is the Apex Body for Disaster Management in India and is responsible for creation of an enabling environment for institutional mechanisms at the State and District levels. NDMA envisions the development of an ethos of Prevention, Mitigation and Preparedness and is striving to promote a National resolve to mitigate the damage and destruction caused by natural and man-made disasters, through sustained and collective efforts of all Government agencies, Non-Governmental Organizations and People's participation.

11 Standardization, Testing and Quality Certification (STQC) Directorate

STQC is a part of Department of Information Technology and is an internationally recognized Assurance Service providing organization. STQC has established nation-wide infrastructure and developed competence to provide quality assurance and conformity assessment services in IT Department Of Information Technology National Cyber Security Policy "For secure computing environment and adequate trust & confidence in electronic transactions " National Cyber Security Policy, draft v1.0, 26 Mar 2011 20

Sector including Information Security and Software Testing/Certification. It has also established a test/evaluation facility for comprehensive testing of IT security products as per ISO 15408 common criteria security testing standards.

12 Sectoral CERTs

Sectoral CERTs in various sectors such as Defence, Finance (IDRBT), Railways, Petroleum and Natural Gas, etc., would interact and work closely with CERT-In for mitigation of crisis affecting their constituency. Sectoral CERTs and CERT-In would also exchange information on latest threats and measures to be taken to prevent the crisis.

Bibliography

- **Books**

Sr. No.	**Books**
1.	Abdul Rahman Garuba – Information Science reference-Security and software for cybercafés, ISBN 978-1-59904-905-2 (e-book)
2.	Barry Nance, Introduction to networking, ISBN: -81-203-1386-0, 1998
3.	Bernard Menezes, Network Security and cryptography, ISBN-13:978-81-315-1349-1, ISBN-IO:81-315-1349-1, 2011
4.	Bruce Anderson & Chris Anderson, Winning the war on internet Defamation, ISBN: 978-0-9859974-0-3
5.	Chawala Deepak and Sondhi Neena, Research Methodology concepts and Cases, Vikas Publication, ISBN 978-81-259-5205-3, 2011
6.	Cheswick William R., Steven M. Bellovin and Aviel D. Rubin, Firewalls and Internet Security , Published by Addison-Wesley Professional , Second Edition, ISBN: 0-201-63466-X
7.	Chuck Easttom,Computer Security Fundamentals, SBN-13: 978-0-7897-4890-4
8.	D.Israel, Data Analysis in Business Research, ISBN:978-81-7829-875-7(PB), 2008
9.	Darlington Onojaefe and Marcus Leaning, Information Science reference - ISBN=1599049058
10.	Detmar W.Straub, Seymour Goodman, Richard L.Baskerville, Information Security Policy, Processes and Practices, ISBN-978-81-203-3745-9, 2009
11.	HM-Treasury, The Orange book – The Management of risk- Principle and Concept, ISBN-1-84532-044-1,
12.	Jennifer L.Bayuk & Jason Healey, Cyber security policy guide book, ISBN 978-1-118-027806,2012
13.	JohnE.Canavan, Fundamentals of Network Security, ISBN 1-58053-176-8, 2000
14.	Kenneth Geers, Strategic Cyber Security, ISBN 978-9949-9040-6-8 (epub), 2011

15. Kothari C.R.,“Research Methodology, Methods & Techniques”, New Age International Publication, New Delhi.

16. Lawrwnce C. Miller, Cyber Security for Dummies, ISBN: 978-1-118-82038-4 (ebk), 2014

17. Michael Ligh, Greg Sinclair, Blake Hartstein, Shahan Sudusinghe, Jon Gary, Robert Falcone, Aldrich De Mata, Ryan Smith, Arion Lawrence, Cyber security Essentials, ISBN 13: 978-1-4398-5126-5, 2011

18. Nandan Kamath : “Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, *ISBN*-13: 978-817534603, 2000

19. P.L.Bhandarkar, T.S.Wilkinson, Methodologies and Techniques of Social Research, ISBN: 978-81-8488-666-5, 2010

20. P.W.Singer & Allan Friedman, Cyber Security and Cyber War, ISBN 978–0–19–991809–6,2014

21. Peter Gottschalk, Policing Cyber Crime, ISBN: 978-1-118-82038-4 (ebk),2010

22. R.K. Chaubey : “An Introduction to Cyber Crime and Cyber Law, *ISBN*: 9350353938,2014

23. Rodney D. Ryder , “Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet, *ISBN-13* : 9350350866, 2011

24. Roger S.Pressman, Software Engineering – A practitioners approach, ISBN 0-07-118458-9, 2001

25. Samuel Samuel Chiedu and Avemaria Utulu – Information Science reference-Security and software for cyber cafes-ISBN 978-1-59904-905-2 (e-book)

26. Tanenbaum Andrew S., Computer Networks, Published by Prentice Hall; 3rd edition (March 6, 1996), ISBN-10: 0133499456

27. V.D. Dudeja , Cyber Crime and the Law, *ISBN* 13: 9788171697090

28. Vakul Sharma, Information Technology: Law and Practice”, ISBN: 9789350350003, 2012

29. Willam Stallings, Cryptography and network security, ISBN 13: 978-0-13-609704-4

- **Journal and Magazines**

Sr. No	**Journal and Magazines**
1	Adomi Eshaenana E., “The Journal of Community Informatics”, http://ci-journal.net/index.php/ciej/article/view/322/319,2007
2	Anikar M. Haseloff - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 - http://ci-journal.net/index.php/ciej/article/view/226/181 - 12/5/2014
3	Asdaque Muhammad Musaud, Khan Muhammad Nasir , Dr.Syed Asad, Rizvi Abbas, “ Journal of Education and Sociology”, ISSN: 2078-032X, December, 2010
4	Cyber Crime the Upcoming Challenge - Sudan Vision – Independence Daily by Muawad Mustapha Rashid July 11 2007
5	Ericsson Goran N. IEEE- “ Transactions On Power Delivery”, VOL. 25, NO3, July 2010
6	Furuholt Bjorn, Kristiansen Stein, “The Journal of Community Informatics”, www.ci-journal.net/index.php/ciej/article/download/314/352 - 2007, ISSN: 1712-4441
7	Gadge Reena K., Dr. Meshram B.B.,"Detect and Prevent Threats in Websites"- IJCST-International Journal of computer science and Techno- vo l. 3, Issue 1, Jan. - March 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)
8	Haseloff Anikar M. - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 - http://ci-journal.net/index.php/ciej/article/view/226/181 - 12/5/2014
9	Haseloff Anikar M. “The Journal of Community Informatics ”,IEEE,UNIVERSITY Vol-1 No.3 2005
10	Iyengar Prashant , http://cis-india.org/internet-governance/front-page/ip-addresses-and-identity-disclosures
11	Larss Magnus Frodigh, Per Johansson and Peter -Ericsson - "Wireless ad hoc networking—The art of networking without a network"- http://www.ericsson.com/ericsson/corpinfo/publications/review/2000_04/files/2000046.pdf - 7/3/2013

12 Longe, O.B., Chiemeke, S.C. and Longe F.A, https://www.intgovforum.org/cms/documents/contributions/general-contribution/2008-1/349-longe-o-b-et-al-isp-and-cybercrime-in-nigeria-igf-contributions/file

13 Mostofa Sk. Mamun and Islam Shariful, “Research Journal of Recent Sciences” ISSN 2277 -2502 Vol. 2(3), 53-58, March(2013), http://www.isca.in/rjrs/archive/v2i3/9.ISCA RJRS-2012-421.pdf - Res. J. Recent Sci

14 Mustafa Koç, Ferneding Karen Ann, “The Turkish Online Journal of EducationalTechnology - TOJET”, July 2007 ISSN: 1303-6521 volume 6 Issue 3 Article 9

15 National Institute of Standards and Technology - http://www.nist.gov/cyberframework/upload/cybersecurity-021214-final.pdf. February 12, 2014

16 Obuh Alex Ozoemelem, “Security and Software for Cybercafes”, DOI: 10.4018/978-1-59904-903-8.ch011, http://www.irma-international.org/chapter/vi1ruses-virus-protection-cybercaf%C3%A9s/28536/

17 Odumesi John Olayemi, “International Journal of Sociology and Anthropology IJSA ” , Vol. 6(3),pp.116-125, March, 2014 DOI: 10.5897/IJSA2013.0510 ,ISSN 2006- 988x , http://www.academicjournals.org

18 Otusile Oluwabukola , S. A. Idowu and Ajayi Adebowale-"Overview of Database Architecture and Security Measures – Attacks and Control Methods"-- Asian Journal of Computer and Information Systems (ISSN: 2321 – 5658) Volume 02 – Issue 02, April 2014 - 2/7/2014

19 Phanse Kaustubh and Chaskar Hemant,. Bhagwat Pravin http://www.airtightnetworks.com/fileadmin/pdf/Implementing_DoT_Regulation_on_Wi-Fi_Security.pdf

20 Sain Hemraj i, Yerra Shankar Rao, Pand.T.C, “ International Journal of Engineering Research and Applications (IJERA)”, ISSN: 2248-9622 Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209, www.ijera.com

21	Sey Araba, Coward Chris, Bar François, Sciadas George, Rothschild Chris and Lucas Published Research Report on -Connecting People for Development-Why public access ICTs matter-http://library.globalimpactstudy.org/sites/default/files/docs/Connecting%20people%20for%20development%20Global%20Impact%20Study%20final%202013.pdf
22	Sife. Alfred S -" Internet use behavior of cybercafé users in Morogoro Municipality, Tanzania"- Annals of Library and Information Studies Vol. 60, March 2013, pp. 41-50
23	Smyth Sara M. , "International Journal of Cyber Criminology" Vol 8 Issue 2 July December 2014
24	Syed Shah Alam , Zaini Abdullah and Ahsan Nilufar , "Journal of Internet Banking and Commerce", April 2009, vol. 14, no.1 - http://www.arraydev.com/commerce/jibc/)

- **Conference & Proceedings**

Sr. No	Conference & Proceedings
1	Arthur Kweku K., Olivier Martin S., Hein S. Venter & Jan H.P. Eloff, The Third International Conference on "Availability, Reliability and Security",ISBN- 0-7695-3102-4/08 IEEE, DOI 10.1109/ARES.2008.107
2	Bahl Sanjay , Wali O P and Kumaraguru Ponnurangam, , " Coalition on Internet Safety", Second Worldwide Cybersecurity Summit,WCS 2011, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber- 978-0-615-51608-0/11 ©2011 EWI
3	Carr John , "Children's Charities', " Coalition on Internet Safety", Second Worldwide Cybersecurity Summit, WCS 2011, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 EWI
4	Derrick J. NeufeldRichard, Proceedings of the 43rd Hawaii International Conference on "System Sciences -2010"
5	Govil Jivesh, Govil Jivika , "Electro/Information Technology", 2007 IEEE International Conference Proceeding, E-ISBN :978-1-4244-0941-9 Print ISBN: 978-1-4244-0941-9, -2007
6	Kriz Danielle- Global Cyber Security Policy, Information Technology Industry ,Second Worldwide Cybersecurity Summit WCS 2011 -

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 -EWI

7 Mathew Alex Roney, Hajj Aayad Al, Ruqeishi Khalil Al, International Conference on "Networking and Information Technology", 2010

8 Newmeyer Kevin P. , Second Worldwide Cyber Security Summit, WCS 2011 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 EWI

9 Nitzberg S. D. , " International Symposium on Technology and Society, U.K", Proceedings of the 1997, ISBN:0-7803-5538-5,Volume-1 , http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=822776&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D822776

10 Patki S A.B., S Lakshminarayanan, S.S. Sivasubramanian , Sarma,Proceedings of the 2003 " International Conference on Cyberworlds", (CW'03)0-7695-1922-9/03 $ 17.00 © 2003 IEEE

11 Petra Raisanenhas, Thesis "The Urban Technospace A Study On Internet Cafés In Shanghai", http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1327545&fileOI d=1327546) 2006

12 Ragaswamy Nimmi ,"International Conference on Ethnographic Praxis in Industry" EPIC 2007 Proceedings - EPICZW7,pp 115 127, ISBN 0 97990942 2 02007

13 Rigoni Andrea, NaiFovino Igor , Blasi Salvatore Di , Second Worldwide "Cyber Security" Summit WCS 2011, ISBN: 978-1-4577-1449-8, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 5978795-8-0-615-51608-0/11 ©2011 EWI

14 White Gregory, Granado Natalie ,Proceedings of the 42nd Hawaii International Conference on "System Sciences"– 2009 ,978-0-7695-3450-3/09 $25.00 © 2009 IEEE

- **Reports**

Sr. No	**Reports**
1	Akinola Azeez Paul and Chong Zhanghas, thesis "Evaluate Security on the Internet Cafe", http://www.divaportal.org/smash/get/diva2:608536/FULLTEXT01.pdf
2	Alaeldin Mansour Safauq Maghaireh, Thesis "Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence", http://ro.uow.edu.au/cgi/viewcontent.cgi?article=4404&context=theses - 2009
3	Cyber Crime, Cyber Security And Right To Privacy fifty-Second Fifteenth Lok-Sabha Report http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf
4	Deity published a XII five -year plan on information technology sector Report of Sub-Group on Cyber Security http://deity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf - 2013
5	Department Of Information Technology, http://deity.gov.in/content/national-cyber security-policy-2013
6	Dr.Kumbhar Manisha published thesis on 'A Critical Study of Implication Of E-Governance Services For Effective Communication With Special Reference To Citizens In Pune City '- (2012)(http ://Shoghganga.org)
7	Government of India regulation under ITA- Information Technology Act – 2000 and Information Technology Amendment Act-http://deity.gov.in/content/information-technology-act- 2008
8	Hamid Salim, Cyber Safety: Thesis "A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks " http://web.mit.edu/smadnick/www/wp/2014-07.pdf
9	Information Note on Regulation of Cyber Cafés in The Mainland, Taiwan, Japan, Singapore and Hong Kong http - www.legco.gov.hk/yr01-02/english/sec/library/0102in34e.pdf
10	Kumbhar Manisha - Thesis on " Critical Study of Implication of e-governance Services for effective communication with special reference to Citizens in Pune Citye"-2011

11 Lok-Sabha Published Fifty-Second report standing Committee On information Technology(2013-14) http://www.electroniccourts.in/privacylawsindia/wp-content/uploads/2014/03/Cyber-Crime-Cyber-Security-And-Right-To-Privacy-Fifty-Second-Report-Of-Standing-Committee-On-Information-Technology-2013-14-February-2014.pdf 2/4/2015

12 Ms.Magacha, Thesis "A Framework For Ethical Usage Of ICT Services At Cyber Cafe Using Theory Of Planned Behavior" http://www.kictanet.or.ke/wp-content/uploads/2014/11/Role-of Cybersecurity-on-Citizens-Security-FINAL.pdf

13 National Crime Bureau Ministry of Home Affair- Published report on Cyber Crime In India http://ncrb.gov.in/CD-CII2013/Statistics-2013.pdf

14 Report on Compilation of Existing Cybersecurity and Information Security Related Definitions- October 2014 - Tim Maurer & Robert Morgus- https://www.newamerica.org/downloads/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions.pdf 8/7/2013

15 Report on Guide for Developing Security -Plans for Federal Information Systems - Marianne Swanson Joan Hash Pauline Bowen http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf 7/7/2014

16 Smart cities Report Published by Symantec 2014- 2015 https://eumartcities.eu/sites/all/files/blog/files/Transformational%20Smart%20Cities%20-%20Symantec%20Executive%20Report.pdf

17 Symantec Published a report on Cyber crime -2013 - http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf - 11/10/2013

18 The Bombay Police Act - was published in 1951- http://www.humanrightsinitiative.org/publications/police/bombay_police_act_1951.pdf

19 The Committee Appointed By The Bombay High Court published Report on Cyber Crime–January 30 2002

20 The Information Technology (Amendment) Bill, 2008 As Passed By Lok Sabha On 22.12.2008

21 Zuriani Bt Ahmad Zukariai, Thesis "A Framework For Ethical Usage Of ICT Services At Cyber Cafe Using Theory Of Planned Behavior", (http://etd.uum.edu.my/2815/2/1.Zuriani_Ahmad_Zukarnain.pdf)2011

- **Websites**

Sr. No	**Websites**
1	http://www.internetlivestats.com/internet-users/ - 2012
2	https://en.wikipedia.org/wiki/Pune-7/8/ 2013
3	https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1 8/8/2013
4	http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf
5	http://articles.economictimes.indiatimes.com/2008-07-02/news/27734377_1_cyber-cafes-cctv-cameras-sirsa, PTI Jul 2, 2008, 04.32pm IST 6/8/2013
6	http://articles.economictimes.indiatimes.com/2008-07-15/news/27697952_1_cyber-cafes-sify-naresh-ajwani, Harsimran Singh, ET Bureau Jul 15, 2008, 08.05am IST 14/8/2012
7	http://articles.economictimes.indiatimes.com/2008-12-03/news/27704863_1_terror-links-cafe-krishna-district, PTI Dec 3, 2008, 02.29pm IST
8	http://articles.economictimes.indiatimes.com/2012-12-30/news/36063564_1_cyber-cafes-check-cyber-crimes-cyber-security, PTI Dec 30, 2012, 10.57PM IST, 30/12/2013
9	http://ci-journal.net/index.php/ciej/article/view/226/181 - 12/5/2014
10	http://ci-journal.net/index.php/ciej/article/view/322/319,2007
11	http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011
12	http://cis-india.org/internet-governance/blog/cyber-cafe-rules 4/6/2012
13	http://cis-india.org/internet-governance/front-page/blog/cyber-cafe-rules - 13/12/2012
14	http://cps-vo.org/group/sos/papercompetition 5/5/2013
15	http://cyberlawclinic.org/casestudy.asp 8/4/2012
16	http://ddpolice.gov.in/downloads/miscelleneous/cyber-cafe-rules.pdf(5/9/2012)

17 http://deity.gov.in/content/information-technology-act- 2008

18 http://deity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf - 2013

19 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber - 978-0-615-51608-0/11 ©2011 EWI

20 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=822776&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D822776

21 http://library.globalimpactstudy.org/sites/default/files/docs/Connecting%20people%20for%20development%20Global%20Impact%20Study%20final%202013.pdf

22 http://protectmyinternetcafe.com/category/internet-cafes-in-the-developing-world-find-out-what-happens-when-everyone/ 25/11/2013

23 http://ro.uow.edu.au/cgi/viewcontent.cgi?article=4404&context=theses - 2009

24 http://searchsoftwarequality.techtarget.com/definition/application-security 5/7/2012

25 http://security.stackexchange.com/questions/57976/nowadays-what-is-the-difference-between-cyber-security-and-it-security - 5/7/2013

26 http://timesofindia.indiatimes.com/city/hyderabad/Net-cafe-staffer-held-for-hacking-bank-account-of-customer/articleshow/5357633.cms 7/8/2013

27 http://timesofindia.indiatimes.com/city/pune/Pune-leaves-Mumbai-behind-in-cyber-crime/articleshow/37591665.cms 30/12/2014

28 http://web.eng.fiu.edu/~aperezpo/DHS/Std_Research/EthicalHackingProject.pdf

29 http://web.mit.edu/smadnick/www/wp/2014-07.pdf

30 http://whitepapers.securityweek.com/technology/enterprise_applications/risk_analysis 5/5/2013

31 http://whitepapers.securityweek.com/technology/enterprise_applications/risk_management 4/3/2011

32 http://www.academicjournals.org 5/5/2013

33 http://www.ccaoi.in/UI/links/articals.php?Id=4&action=view 7/7/2013

34 http://www.census2011.co.in 1/1/2013

35 http://www.cert.org 4/4/2012

36 http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html 8/8/2014

37 http://www.csemag.com/single-article/3-pillars-of-industrial-cyber-security/ae9f214bcd0f00fba81c041826a94d34.html 8/3/2012

38 http://www.divaportal.org/smash/get/diva2:608536/FULLTEXT01.pdf

39 http://www.humanrightsinitiative.org/publications/police/bombay_police_act_1951.pdf

40 http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf 9/11/2013

41 http://www.icscybersecurityconference.com/#!call-for-papers/c12k8

42 http://www.imrbint.com/downloads/Report-BB55685%20IAMAI%20ICUBE_2013-Urban+Rural-C1.pdf - 8/8/2013

43 http://www.irma-international.org/chapter/vi1ruses-virus-protection-cybercaf%C3%A9s/28536/ 9/3/2011

44 http://www.isca.in/rjrs/archive/v2i3/9.ISCA RJRS-2012-421.pdf - Res. J. Recent Sci

45 http://www.kictanet.or.ke/wp- content/uploads/2014/11/Role-of Cybersecurity-on-Citizens-Security-FINAL.pdf

46 http://www.legalserviceindia.com/lawforum/index.php?topic=2238.0 7/4/2012

47 http://www.maharashtrafireservices.org/pdf/pune_mitigation_plan.pdf (2/5/2012)

48 http://www.mapsofindia.com/maps/maharashtra/pune.htm (23/7/2010)

49 http://www.nist.gov/cyberframework/upload/cybersecurity-021214-final.pdf. February 12, 2014

50 http://www.punemirror.in/news/india/Cyber-stalker/articleshow/32718227.cms

51 http://www.techsoupforlibraries.org/book/export/html/592 5/7/2013

52 http://www.thehindu.com/news/cities/chennai/testing-time-for-cyber-cafes/article1718950.ece, June 6, 2013 14:22 IST

53 http://www.wipo.int/edocs/lexdocs/laws/en/in/in100en.pdf(12/3/2013)

54 http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf - 11/10/2013

55 https://books.google.co.in/books?isbn=1599049058 3/3/2014

56 https://en.wikipedia.org/wiki/Computer_security - 8/8/2014

57 https://en.wikipedia.org/wiki/Information_security -4/7/2013

58 https://en.wikipedia.org/wiki/System_software 9/9/2013

59 https://eumartcities.eu/sites/all/files/blog/files/Transformational%20Smart%20Cities%20-%20Symantec%20Executive%20Report.pdf 7/3/2015

60 https://www.caida.org/publications/papers/2014/creds2013_report/creds2013_report.pdf 5/7/2012

61 https://www.intgovforum.org/cms/documents/contributions/general-contribution/2008-1/349-longe-o-b-et-al-isp-and-cybercrime-in-nigeria-igf-contributions/file 8/8/2013

62 Internet censorship in Vietnam article https://en.wikipedia.org/wiki/Internet_censorship_in_Vietnam 3/6/2012

63 Internet cyber cafe - https://en.wikipedia.org/wiki/Internet_caf%C3%A9 - 7/7/2012

64 www.ci-journal.net/index.php/ciej/article/download/314/352 - 2007, 8/8/2012

- **News Papers**

Sr. No	**News Papers**
1	Economic Times - 15/06/2008, 3/12/2008, 5/06/2013
2	Maharashtra Times - 9/2/2011
3	Sakal - 8/2/2011, 10/2/2011, 17/2/2011, 26/7/2011, 26/7/2011, 10/07/2011, 18/11/2011, 25/9/2013, 3/10/2013
4	The Hindu - 6/06/2013
5	Times Of India - 18/10/2010, 28/10/2010, 22/11/2010, 22/11/2010, 7/5/2011, 9/5/2011, 6/5/2011, 6/5/2011