Analysis of Cyber Crime in Banking Sector

DISSERTATION

Submitted in the Partial Fulfilment for the Degree of

MASTER IN LAW'S (LL.M.)

2019-2020

BBD UNIVERSITY

Under Supervision of: –

Ms. Sonali Yadav

Assistant Professor

School Of Legal Studies

Babu Banarasi Das

University Lucknow

Submitted by:–

Imtishal Shah

LL.M. II Semester

Babu Banarasi Das

University Lucknow

Roll No.: 1190997022

BABU BANARASI DAS UNIVERSITY

Phone No.: +91-(522)-3911100/01/02
info@bbdu.org
http://bbdu.ac.in
BBD City, Faizabad Road,
Lucknow Uttar Pradesh (INDIA)

DECLARATION

Title of Project report **Analysis of Cyber Crime in Banking Sector.** I understand what plagiarism is and am aware of the University policy in this regard. **Imtishal Shah.**

I declare that:

(a) The work submitted by me in partial fulfilment of the requirement for the award of degree LL.M. Assessment in this DISSERTATION is my own, it has not previously been presented for another assessment.

(b) I declare that this DISSERTATION is my original work. Whatever work from other source has been used, all debts (for words, data argument and idea) have been appropriate acknowledged.

(c) I have not used this work previously produced by another student or any other person to submit it as my own.

(d) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off ass his own work.

(e) The work confirms to the guidelines for layout, content and style as set out in the Regulation and Guidelines.

Date :

Researcher :

IMTISHAL SHSH

ACKNOWLEDGEMENT

Research is a very intricate and challenging enterprise which needs consistent hard work, dedication and constant consultation. Its completion requires the investigator to seek help and guidance at all stage.

First of all my head bows down to 'Almighty God' who has blessed me with the opportunity, skills and capacity to achieve the goal of my life.

Words fall short to express gratitude to my esteemed supervisor Ms. Sonali Yadav, Assistant professor, School of Legal Studies, Babu Banarasi Das University, Lucknow for her constructive criticism, help and generous guidance. I feel very indebted to her for keen interest, untiring help, inspiring, incisive guidance and constant encouragement. She made it possible for me to complete this work.

I am also thankful to the Principals, Teaching Staff. I am also thankful to my batch mates for helping me throughout year.

My acknowledgement will be incomplete if I do not mention my parents with whose blessing I was able to achieve my goal successfully. There are no words to express my feelings toward them. I silently acknowledge my debt to them.

.Solemnly claims all the responsibility for the errors and omissions in this work.

IMTISHAL SHAH

ABBREVIATIONS

ACPA	**Anti- Cybersquatting Consumer Protection Act**
ATM	**Automated Teller Machine**
CSS	**Cross-Site Scripting**
CVV	**Card Verification Value**
DDoS	**Distributed Denial of Service**
DOD	**Department of Defence**
EFT	**Electronic Funds Transfer**
HTML	**Hyper Text Markup Language**
HTTP	**Hyper Text Transfer Protocol**
IT	**Information & Technology**
ICT	**Information and Communication Technology**
ICICI	**Industrial Credit and Investment Corporation of India**
ISO/IEC	**International Organization for Standardization/ International Electrotechnical Commission**
IDBI	**Industrial Development Bank of India**
MMS	**Multimedia Messaging Service**
MIT	**Man in the Middle Attack**
MITB	**Man in the Browser Attack**
MITPC	**Man in the Personal Computer Attack**

NCRB	**National Crime Record Bureau**
NEFT	**National Electronic Fund Transfer**
NGN	**Next Generation Network**
PNB	**Punjab national Bank**
RBI	**Reserve Bank of India**
RTGS	**Real Time Gross Statement**
SBI	**State Bank of India**
SMS	**Short Message Service**
SSL	**Secure Stockets Layer**
SWIFT	**Society for Worldwide Interbank Financial Telecommunication**
VoIP	**Voice over Internet Protocol**

TABLE OF CONTENT

CHAPTER – I

INTRODUCTION

CHAPTER – I

INTRODUCTION

1.1. Introduction:

Cybercrime is emerging as a challenge for national and economic security. Many industries, institutions and public and private sector organizations (particularly those within the critical infrastructure) are at significant risk. Comparatively some organizations have identified organized cybercriminal networks as its most potential cyber security threat and some are ready to defend such security threats. The complexity of modern enterprises, their reliance on technology and the heightened interconnectivity among organizations have created widespread opportunities for theft, fraud and other forms of exploitation by offenders both outside and inside an organization. With the growth of e-business, internal and external perpetrators can exploit traditional vulnerabilities in seconds. They can also take advantage of new weaknesses in the software and hardware architectures that now form the backbone of most organizations. In a networked environment, such crimes can be committed on a global basis from almost any location in the world, and they can significantly affect an organization's overall work culture. Network and computer attacks have become common issues in today's world. Any computer connected online is under threat from viruses, worms and attacks from hackers. Public users as well as business users are attacked on a regular basis.

Cybercrimes have practically no boundaries and may affect every country in the world. Mounting Cybercrimes across the world is a very stern warning in the up-coming time and produces one of the most complicated challenges before the law enforcement machinery.

Online banking or e-banking refers to the banking facility through information and communication technology. Traditionally, banking required a customer to stand in a long queue even to withdraw his money or to perform other ancillary functions. Now banking facility is available 24×7 through ATMs (Automated Teller Machines), internet banking,

transfer through NEFT and RTGS etc., which has narrowed down the gap between the bank and the customer. E-banking is not only limited to banking facility through computer related systems. In the modern era, with the increase of users of smartphones e-banking covers mobile banking also. Because of liberalization, privatization and globalization, it became necessary for the banks to start with e-banking facility. The paper will provide an introduction to the concept of e-banking and its advantages in India. Further the author will provide statistics of the increase in use of e-banking services in India. The paper shall also highlight the role of Reserve Bank of India in strengthening internet banking. The paper shall then delve into the drawbacks of e-banking by explaining various cyber-crimes related to banking, focusing on Information Technology Act, 2000 with the help of statistics on cyber-crime reported in the past few years.

Economy is one of the pillars which defines the progress and growth of a nation. Banking sector is considered as the backbone of the economy. For our day-to-day transactions, we enter into monetary transactions in the form of cash payments, cheques or demand drafts. However, this trend has paved the way to a modern system of payment in the form of swiping of debit cards or credit cards. On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998, information and technology in banking sector was used. On one hand, technology has created advantage for banks and financial institutions but on the other hand, there have been risks involved in it as well. Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information. Banking sector has witnessed expansion of its services and strives to provide better customer facility through technology but cyber-crime remains an issue. Information which is available online is highly susceptible to be attacked by cyber criminals.4 Cyber-crimes result in huge monetary losses which are incurred not only by the customer but by the banks also which affects economy of a nation. Non-monetary cyber-crime occurs when viruses are created and distributed on other computers or confidential business information is posted on Internet. The most common of it is phishing and pharming.

1.2. Cyber space:

Today, the word “cyberspace” is used in many contexts, but it is not always clear what exactly that term describes and what it means. The term “cyberspace” is such that all other terms (e.g., cyber security, cybercrime, cyber war, cyber terrorism, etc.) are based on, or derived from, cyberspace itself. Therefore, cyber security is security of cyberspace. Cybercrime is a crime that is committed within cyberspace or where element from/of cyberspace are used as a vehicle to commit a crime, and so on for other derived terms.

In Order for a definition to be considered for inclusion into the research a definition must satisfy two conditions: it must have an official definition and it must be made by a respectable entity. For this purpose, we define “official” as being presented in a high level document that is used as the basis for developing policies and is prevalent for a given organization/region. Entities like government and standardization setting bodies are considered to be respectable in a sense that they influence the thinking and behaviour of a multitude of organizations.

The list of governments and organizations whose definitions of cyberspace have been identified as official and authentic are as follows:

According to Oxford English Dictionary, 2009 Edition,

“The space of virtual reality; the nation environment within which electronic communication (esp. via the Internet) occurs.”

According to Canada, Canada’s Cyber Security Strategy, 2010,

“Cyberspace is the electronic world created by interconnected network of information technology and information on those networks. It is a global common where more than 1.7 billion people are linked together to exchange ideas, service and friendship.”

According to Netherlands, The National Cyber Security Strategy

"Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information."

According to Germany, Cyber Security Strategy for Germany, 2011,

"Cyberspace is the virtual space of all IT system linked at data level on a glob scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace."

According to New Zealand, New Zealand Cyber Security Strategy, 2011,

"The global network of interdependent information technology infrastructures, telecommunications networks and computer processing system in which online communication takes place."

According to United Kingdome, The UK Cyber Security Strategy, 2011,

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information system that supports our businesses, infrastructure and services."

According to United States, National Security Presidential Directive 54/Homeland Security Presidential Directive, 23, 2008,

"Cyberspace is defined as the interdependent network or information technology infrastructures, and includes the Internet, telecommunications networks, computer systems and embedded

processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."

According to ITU, ITU-T Recommendation Rec. ITU-T X.1205 (X.cso) 2008,

"Technologies, such as wireless networks and voice-over-IP (VoIP) extend the reach and scale of the Internet. In this regard, the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can be connected directly or indirectly to the Internet, and to the next generation network (NGN) environment, latter with public and private incarnations. Thus, with VoIP technology, a desk telephone is part of cyber environment if they can share information with connected computing devices through removable media. The cyber environment includes the software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices, Installations and buildings that house the devices are also part of the cyber environment."

According to ISO/IEC, ISO/IEC 27032 Guidelines for Cyber Security (Draft) 2011,

"The Complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

Based on the keywords and categories extracted from the definition to understand cyberspace in a more comprehensive manner we can construct the following table that shows how and where definitions differ from each other without questioning the validity of the definition of cyberspace, we can make the following confirmations based on the information presented in the above definitions:

	Tangibles		Intangibles					Network Related		
	ICT 1	HW	Information 2	Activities	App. Service	Social Human	Virtual	Internet	Network	Interconnectivity
Oxford Dictionary							√	√		
Australia*	√	■	■							
Canada	√	■	√		√	√	√		√	√
Germany	√	■	√				√	√	√	√
The Netherlands*	√	■	■							
New Zealand	√	√							√	√
The U.K.			√	√	√	√	■	√	√	
The U.S.A.	√	√	√	√		√	√	√	√	√
The E.U.		√	√				√			
ISO		√	√	√	√	√	√	√	√	√
ITU		√	√		√	√	√	√	√	√

Table 1: Element of various cyberspace definitions an overview.

[1]Hardware encompass items like: computer, PC, processor, controller, etc.

[2]Information includes signalling (i.e. communication between processor and/ or devices) but also the content of the exchange.

√ The definition explicitly references this element.

■ The definition implicitly references this element.

* Derived definition. There was no direct definition of cyberspace so its meaning was derived from other definition (mostly commonly from cyber security).

From the careful observation of the above table we can figure out how and where definition differ from each other without questioning the validity of the definition of cyberspace, we can make the following conclusions based on the information presented in the table above:

- Virtually all definitions agree that cyberspace includes tangible elements. This would imply that cyberspace cannot exist without tangible elements.
- Virtually all definitions agree that cyberspace must include information. Information can either be stored data, signalling between processes and/ or devices or as a content that is being transmitted.
- Cyberspace includes tangible but, at the same time, it is also virtual.
- Probably contrary to popular beliefs, networks and Internet are not necessarily part nor are required for cyberspace but they are still 'desired'. Interconnectivity seems to have an equal weight as the Internet itself.

1.3. Cyber Literacy:

Cyber Literacy is the ability to use computer technologies effectively and to simultaneously understand the implications of those actions. It is important to know where to go to find reliable and accurate resource in cyberspace.

Cyber literacy, in the broad understanding means more than just being able to use the technology but to have a consciousness of one's actions.

Examples of cyber literacy include:

- Being able to judge the legitimacy of a website.
- Safe searching/ downloading practices against viruses and phishing scams.
- Being able to follow and interact with non-linear conversation through posts.
- Knowing which information you can and can't safely put onto social networking sites.

- Being aware of this time in space and the consequences.

- An electronic literacy, not just a computer literacy.

- A consciousness of what we are doing online and motivations.

- Reach, anonymity, interactivity, speed.

1.3.1. Principle of cyber literacy

There are mainly three principle of cyber literacy-

1. **Cyber space has no restrictions.**
2. **Cyber space keeps everything recorded.**
3. **Cyber space imposes challenges on "individuality".**

1. Cyber space has no restrictions

Cyber space is an artificial space supported by technologies and has no restrictions in principle unless introduced intentionally. As Cyber space is seamless both spatially and temporally, it is possible that an entertainment district is adjacent to a court and people around the world communicate with each other. Additionally, a digital copy is identical to an original and yet the quality will not be deteriorated even after repeated copy operations. It is not attenuated or worn away while being transmitted long way. Cyber space has no "ambiguity", "incompleteness", "attrition", "physical hazard", "self-stabilizing", and "natural order" that we can find in the real world. And it is also this characteristic of digital information which enables us to strictly regulate

and control information which enables us to strictly regulate and control information. That is a cause of various problems we have lived with in modern society.

2. Cyber space keeps everything recorded

We have been contributing to build a huge database of personal information by volunteering personal data when we make payment at shops, deposit money in a bank, or use public services (for driving licenses or tax payment). Even e-mail messages sent from computers and mobile phones remain on the network permanently unless every effort is made to "delete" them.

3. Cyber space imposes challenges on "individuality"

Too much dependability on cyber technology is making a sense of belongingness to traditional communities became weaker and weaker. Of course this technology can be used to foster communicating among families, but it is because you intended to do so. The most important thing is that people are inevitably challenged at an "individual" level. One might say that Cyber space exposes "individuals" to situation where they are challenged and tested. Those "individuals" thrust out bare and alone are in danger of being taunted, manipulated, or controlled by cyber space. Even so, they also have a good chance of tacking advantage of Cyber space to establish their own autonomous networks. This is again left to the discussion of individuals.

1.4. Knowledge of cybercrime, cyber space and cyber ethics

1.4.1. Cybercrime

Cybercrime or computer oriented crime is a crime that involves a computer and a network. The computer may have been used in the common of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental

harm, or loss, to the victim directly and indirectly, using modern telecommunication network such as Internet (networks including but not limited to Chat rooms, e-mails, notice board and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrimes may threaten a person or a nation's security and financial health. Issues surroundings these types of crimes have become high-profile, particularly those surroundings hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Further cybercrime from the perspective of gender and define 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interest of at least on nation's state is sometimes referred to as Cyberwarafare.

Various types of cybercrimes are listed as follows:

1. Fraud and Financial Crimes

A computer fraud is any dishonest misrepresentation of fact indeed to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Alternative in an unauthorized way. This requires little technical expertise and is common form of theft by employees alternating the data before or entering false data, or by entering unauthorized instructions or using unauthorized process.
- Alternating, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect.
- Alternating or deleting stored data.

Other forms of fraud may be facilitated using computer system including bank fraud, carding, identity theft, extortion, and theft of classified information. A variety of internet scams, many based on phishing and social engineering, target consumers and businesses.

2. Cyber Terrorism

Cyber Terrorism is generally can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyber terrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstration power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

3. Cyber Extortion

Cyber-extortion occurs when a website, e-mail server, or computer system is subjected to do threaten with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection".

According to Federal Bureau of Investigation, cyber-extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. An example of cyber extortion was the attack on Sony Pictures of 2014.

4. Cyber warfare

The U.S. Department of Defence (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those area included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russian again allegedly conducted cyber-attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by war fighting military commanders in the future.

5. Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as computers have – which explains how unprepared society and the world in general is toward combating these crimes. These are numerous crimes of this nature committed daily on the internet, crimes that primarily target computer networks or devices include:

- Computer Viruses
- Denial-of-service attacks
- Malware (malicious code)

6. Computer as a tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend. The unsolicited sending of bulk email for commercial purpose (spam) is unlawful in some jurisdictions. Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware. Or, they may contain links of fake online banking or other websites used to steal private account information. Crimes that use computer networks or devices to advance other ends include:

- Frauds and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both “computer as target” and “computer as tool” crime)
- Information warfare

- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and treats.

7. Obscene or Offensive content

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances, these communications may be legal. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs. One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

8. Harassment

Various aspects needed to be consider when understanding harassment online, content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focussing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties.

Harassment on the Internet also includes revenge porn. Harassment as defined in the U.S. computer statute is typically distinct from cyber bullying, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act" while the later need not involving anything of a sexual nature.

9. Drug Trafficking

Drug net markets are used to buy and sell recreational drug online.

Some drug traffickers use encrypted messaging tool to communicate with drug mules. The dark web sites Silk Road was a major online marketplace for drug before it was shut down by law enforcement (then reopened under new management, and then shut down

by law enforcement again). After Silk Road 2.0 went down, Silk Road 3.0 Reloaded emerged. However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.

1.4.1.2. Countering cybercrime and related measures

1. Diffusion of Cybercrime

The broad definition of cybercriminal activities is an issue in computer crime detection and prosecution, technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, Hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skill in server management, network configuration, and maintenance, knowledge of Internet service provider standard, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk and transactional e-mail-service for making for marketing purpose and could be easily set up for spam. Could computing could be helpful for a cybercrime as a way to leverage his attack – brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign.

2. Investigation

A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for crime purpose, it may contain records of value to criminal investigation in the form of a log file. In most countries Internet Service Providers are required, by law, to keep their log files for a predetermined amount of time. For example; A European wide Data Retention Directive (applicable to all EU member state) states that all E-mail traffic should be retained for a minimum of 12 month. There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace; however that is not necessarily a factual basis upon which detectives can solve a case. Different type of high-tech crime may also include elements of low-tech crime, and vice-versa, making cybercrime investigators an indispensable part of modern law-

enforcement. Methodology of cybercrime detective work is dynamic and is constantly improving, whether is closed police units, or in international cooperation framework.

3. Legislation

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution form law enforcement. In developing countries, such as India, laws against cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allows for prosecution. While this proves difficult in some cases, agencies, such as FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United State by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.

4. Penalties

Penalties for computer related crimes can range from a fine and a short period of jail time for a Class A misdemeanour such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison. However, some hacker have been hired as information security expert by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the Internet or computers, even after they have been released from prison – though as computer and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyber offender behaviour without resorting to total computer or Internet bans. These approaches involve restricting individuals to specific devices which are subject to computer monitoring or computer searched by probation or parole officers.

5. Intelligence

As cybercrime has proliferated, a professional ecosystem has evolved to support individuals and groups seeking to profit from cybercriminal activities. The ecosystem has become quite specialized, including malware developers, botnet operators, professional cybercrime groups, groups specialized in the sale of stolen content, and so forth. A few of the leading cyber security companies have the skills, resources and visibility to follow the activities of these individual and group. A wide variety of information is available from these sources which can be used for defensive purposes, including technical indicators such as hashes of infected files or malicious IPs/URLs, as well as strategic information profiling the goals, techniques and campaigns of the profiled groups. Some of it is freely published, but consistent, on-going access typically requires subscribing to an adversary intelligence subscription service.

6. Agencies to counter cybercrime

Main agencies across the globe to counter cybercrime are as follows:

- Australian High Tech Crime Centre, Australia.
- Cyber Crime Investigating Cell, a wing of Mumbai Police, India.
- Cyber Crime Unit (Hellenic Police), Greece.
- National White Collar Crime Centre, United States.

1.4.2. Cyber Security

Cyber security or cyber safety, a common term used to describe a set of practices, measures and/ or actions that protect technology and information from attacks, is a hot topic in business these days. Every company (whether large or small) or a group/ individual is a target for cybercrime, and being prepared and vigilant has become an absolute necessity. Most common issues span five basic categories:

- Viruses, which infect computer through e-mail attachments and file sharing, can delete files, attack other computer and make system run slowly.

- Hackers are people who “trespass” into computer from remote locations. They can then cause the breached machine to malfunction, or use it to host to host a website, and send spam or spread viruses.
- Identity thieves obtain unauthorized access to personal information, such as social security and financial account numbers. They can then use this information to commit crimes such as fraud or theft.
- Spyware, which is software that piggybacks on programs that are downloaded, gather information about a user’s online habits and transmits personal information without their knowledge.
- Ransomware is a more recent – and rapid going – threat. Perpetrators restrict access to software programs and files, most often by encrypting them, and then demand that the users pay a ransom to remove the restriction.

These issues are serious, and they are becoming more prevalent. Symantec, a cyber-security tool provider, report that security breach increased by 23 percent in 2017. More than 317 million new pieces of malware were created, averaging to nearly 1million new threat each day.

General basic seven actions (In most cases, the implementation of these security measures takes only a few minutes) that helps protect computers and data are as follows:

1. Install OS/ software updates: Updates, sometimes called patches, fix problem with an operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS X) and software programs (e.g., Microsoft Office applications). Most new operating system is set to download updates by default. After updating are downloaded, users are asked to install them click yes!

2. Run anti-virus software: To avoid computer problem caused by viruses, installed and run an anti-virus program like Norton, a product from Symantec. Periodically, check to see if the anti-virus is up to date by opening the anti-virus program and checking the date of the last update.

3. Prevent identity theft: Never give out financial account number, Social Security number, driver’s license numbers or other personal identity information unless recipient is known. Never send personal or confidential information via email or instant messages, as these can be easily intercepted. Beware of phishing scams – a form of frauds that uses email messages that appears

to be from a reputable business (often a financial institution) in an attempt to gain personal or account information.

4. Turn on Personal firewalls: Check computer security settings for build-in personal firewalls – and turn them on. Firewalls act as protective barriers between computer and the Internet. Hackers search the Internet by sending out pings (calls) to random computer and wait for responses. Firewalls prevent computers from responding.

5. Avoid spyware/ adware: Spyware and adware take up memory, and can slow down computers and cause other problem. Using Spybot and Ad-Aware to remove spyware/adware. Both of these programs are available online for free.

6. Protect passwords: Never share passwords. Establish a computer "safe word" that a support technician requesting your work system login must known. Not to use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, (your name)1, baseball 1. Change your password periodically. When choosing a password, mixing upper and lower case letter and use minimum of eight characters.

7. Back up important files: Reduce the risk of loosing important files to a virus, computer crash, theft or disaster by creating back-up copies. Store back-up media in a secure place away from your computer, in case of fire or theft. Testing back-up media periodically to make sure the files are accessible and readable.

Implementing these measures and staying on top of them can go a long way toward helping users fight common cyber security threats and the resulting consequences.

1.4.3. Cyber Ethics

Cyber ethic is the study of ethics pertaining to computers, covering user behaviour and what computer are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have explained policies about cyber ethics.

With the increase of young children using the internet, it is now very essential than ever to tell children about how to properly operate the internet and its dangers. It is especially hard to talk to teens because they do not want to be lectured about what is right and wrong. They seem to think

they have it all sort out. That is way is it is important to in still appropriate cyber etiquette at an early age but if you haven't there is still time to tell them.

Cyber ethics include the following factors:

1. Following copyright rules.
2. Giving a copy-paste culture.
3. Academic honesty (Giving credit to author).
4. Using the information in legal way.
5. Respecting the privacy of others.
6. Keeping up passwords private.
7. Avoiding the use of offensive language online.
8. Keeping an eye at online strangers.
9. Do not disclose personal information to online strangers.
10. If found something suspicious contact cyber cell.

1.4.3.1. Aspects of Cyber ethics

1. Responsible Behaviour on the Internet

Cyber ethics concern to the code of responsible behaviour on the Internet. Just as we are taught to act responsible in everyday life. The responsible behaviour on the internet in many ways aligns with all the right behaviour in everyday life, but the result can be significant different.

Some people try to hide behind a false sense of obscurity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them. That is not all the time true; browsers, computers and internet service providers may keep long of their activities which can be used to spot illegal or inappropriate behaviour.

The government has taken a positive role in making resources for parents and children to learn about cyber ethics. This is a growing problem and without parents and teacher using the resources available nothing can be done to prepare future generations of internet users from being safe online.

2. Copyright and Downloading

Copyright or downloading is a major issue because children don't know copyright policies. They only try to search what they need from the web and download it for their purpose. Their thinking is like "if everybody is doing it therefore it's ok", but an understandable and an age appropriate lesson on Cyber Ethics could help children to learn the risk involved in internet downloading.

3. Crime and Punishment

Children do not believe that they will get into real problem from neglecting the use of cyber ethics. It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust. The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions. In India government has also started taking appreciable measures regarding the issue.

4. Internet Hacking

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computer it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make individuals aware by telling its importance.

5. Cyber-bullying

Cyber bullying is increasingly and people are become aware of its effects on children. Cyber bullying is bullying that takes place carrying electronic technology. Electronic technology carried by devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, website and chat.

When a user encounters cyber bullying he/she should:

- Tell a trusted authority, and keep telling them until they take action.

- Avoid to open, read or respond to messages from cyber bullies.
- Always keep messages from bullies. They may need to take corrective action.
- Use software to block bullies if they encounter them through chat or IM.

Use of technology by people if globally accepted as it facilitates the searching and retrieval of information needed for their academics and consequently the successful completion of their education programs. They need to be aware and knowledgeable about the ethics surrounding the use of ICT is therefore, equal important. Student must be aware and possess the knowledge about cyber ethics. Therefore, cyber ethics education must be provided to students by the school and college.

1.5. Need of the Study

Banking industry has gone through major changes in recent past. Almost all the banks in India have adopted Information Technology solutions for rendering the banking services to their customers by using the IT tools & techniques to fulfil the needs of the customers. Due to the dawn of e-banking, conventional banking has been disappeared from the Indian banking scenario and banks have shifted from traditional banking to Core Banking Solution. Under these circumstances Indian banking industry is facing the challenges of impact of technology on the banking. In the age of information technology the swift expansion of, telecommunications, computers and other technologies has led to the new forms of crimes known as “Cyber Crimes”. Cybercrime doesn’t know the physical boundaries and may affect every country in the world. The transformation in committing crimes with the help of information technology; the law should not be a mute spectator but to transform itself according to the changing environment. There was a need to redefine the old laws in the changing environment. Most of the existing laws in India are either created by the British Government or enacted after the independence within the first three decades and based on physical environment, geographical boundaries, tangible documents and records. In the digital era, everything is recorded in digits, irrespective of any physical boundaries. Due to these consequences there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. Under these circumstances, E-Commerce Act, 1998 was enacted. After two years of passing of this law, Indian parliament passed “Information Technology Act, 2000” on 17th Oct 2000 to have its

exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties & punishments in the field of cybercrimes.

As technology advances and more people rely on the internet to store sensitive information such as banking credit card information, criminals are going to attempt to steal that information. Cyber-crime is become more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world. According to FBI's Internet Crime Complaint Centre in 2017 there were 269,422 complaint filed. With all the claims combined there was a reported total loss of $800,492,073. But yet cyber-crime doesn't seem to be on average person's radar. There are 2.5 million cyber-attacks annually across the globe, which means that there are over 6850 attacks a day, 285 every hour, or nearly 12 attacks every minute, with studies showing us that only 16% of victims had asked the people who were carrying out the attacks to stop. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online. Height of wrongdoing occurring in banking sector have focused that there is need to study the scenario of cybercrimes in India. It is an emergence need to control it by best options.

1.6. Statement Of Problem

The Purpose of the study to cover the aspect of control of cybercrimes against the banking sector. This study is an attempt to evaluate up to what extent cybercrime affects the banking. Similarly the researcher has made an attempt through this research work to analyse the cyber-crime in Banking.

1.7. Operational Definitions

Cybercrime is a crime that is peruse through the virtual network by the electronic devices like computer, laptop, mobile phones with an intention to commit fraud, steal identity, gain monetary value, and breach privacy etc.

1.8. Objective of the Study

1. To study the working operation of cybercrime.
2. To study technique used in cybercrime in banking sector.
3. To Study meaningful analysis of the data belonging to banking cybercrime of different banking sectors.
4. To study the current status of cybercrimes in banking sector.
5. To identify the preventive measures to control frauds.

1.9. Hypothesis of the Study

1. There exists complex networking of cyber-crime.
2. There are so many ways to fraud.
3. There is acute problem of cyber-crime in banking sector.
4. Fourth object has no hypothesis it is based on reviews and own study.
5. There exist so many laws and preventive rules for cybercrime in banking sector.

1.10. Review of Literature

1.10.0. Studies Reviewed for the Present Study

1.10.1. United States

2012: As a result of cyber-crime reported by New York Times, "Frustrated customers of Bank of America, JPMorgan Chase, Citigroup, U.S. Bank, Wells Fargo and PNC, who could not get access to their accounts or pay bills online, were upset because the banks had not

explained clearly what was going on". Furthermore, "CEO Brian Moynihan told analysts the bank of America is spending "hundreds of millions of dollars a year" on cyber security to guard against data breaches". The aim of attackers was not to gain a financial advantage/theft but to frustrate the customers that could ultimately cause a financial loss to the institutions. As reported by CNN, "Denial of service attacks is an effective but unsophisticated tool that doesn't involve any actual hacking. No data was stolen from the banks, and their transactional systems like their ATM networks remained unaffected. The aim of the attacks was simply to temporarily knock down the banks' public-facing websites.

2014: USA Today reports, "Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building".

2016: Another news reports, "Forty-six major financial institutions were targeted with distributed denial of service (DDoS) crimes in which hackers gain remote control of hundreds of computers and servers and use them to flood a target's server with data, clogging it up so that it can't receive legitimate traffic". Furthermore, NBC news says "Targets included Bank of America, the New York Stock Exchange, Capital One and ING, and PNC Banks, according to court papers". In addition to the above, "FBI and US secret service agents have arrested a man charged with the largest cyber-attack of financial firms in America's history. The company hit hardest by the breach was JPMorgan. More than 83 million of the bank's customers had data stolen in the breach.

1.10.2. Europe

2015: "The RBS banking group has revealed it suffered a cyber-crimes on its online services that left customers struggling to log on for nearly an hour – just as monthly pay cheques were arriving in accounts".

In late **2015**, several incidents of cyber-attacks took place in online trading as mentioned by NASDAQ, "The latest data breach was reported by FXCM Inc. FXCM , an online foreign exchange trading and related service provider, on Oct 1. According to the company, hackers gained unauthorized access to customer information and a few transfers were made from certain accounts".

An Information Security Company Group-IB published in a blog," In February 2015, for the first time ever, a Trojan dubbed Corkow (Metel) gained control of a stock exchange trading terminal and placed orders worth a total of several hundred million dollars. In just 14 minutes attackers created abnormal volatility, which made it possible to buy dollars for 55 rubles and sell them for 62 rubles. As a result of the incident, a Russian bank suffered huge losses, although it was random traders rather than the hackers themselves that profited from it".

In February 2016, hackers tried to steal $951 million from the Central Bank of Bangladesh via the SWIFT system. This company highlighted that cybercrimes does not cause only financial loss or information breach but it can also be used in spying and cyberterrorism. Corkow is also known as Metel.

2016: In another report by Crime Russia, "Hackers from the Lurk team, which created the banking Trojan of the same name, were able to steal more than 1.7 billion rubles ($28.3m) from the accounts of Russian banks before being detained by the Interior Ministry and the FSB in June 2016". Crime Russia highlights the case of Energobank where Metel's attack caused the bank damages of 244 million rubles ($3.7M). The Kaspersky written in a blog," One way or another, the criminals stripped each victim bank of $2.5 million to $10 million – the amount looks striking even when assessed individually".

Buhtrap is another cyberattack. "Experts estimate that the lowest amount stolen from a Russian bank is $370,000 (25 million RUB), and the highest amount is close to $9 million (600 million RUB)".

2017: HSBC one of the largest bank in world as well as in Europe suffered from a cyber-crime in early 2017. A report from The Week Newsletter stated, "HSBC customers were unable to access

online banking services for the second time in a month today, in the wake of an apparent cyber-crime".

1.10.3. Asia

2010: Umashankar Sivasubramaniam Vs ICICI Bank is one of the famous phishing fraud case. According to Economic Times," In a verdict in the first case filed under the Information Technology Act, Tamil Nadu IT secretary on Monday directed ICICI Bank to pay Rs.12.85 lakh to an Abu Dhabi-based NRI within 60 days for the loss suffered by him due to a phishing fraud".

2016: "ICICI Bank, HDFC Bank and Axis Bank - the top three private sector lenders - confirmed in separate statements some of their customers' card accounts had been possibly breached after use at outside ATMs".

According to Crime Russia, "Another group, purposefully attacking banks, is Lazarus, the most famous theft of $81 million from the Bangladesh Bank in 2016". Further it stated by Group-IB, In February 2016, hackers tried to steal $951 million from the Central Bank of Bangladesh via the SWIFT system. This company highlighted that cybercrime does not cause only financial loss or information breach but it can also be used in spying and cyber terrorism. Corkow is also known as Metel . In another incident of cyber-crime in Turkey Insurance Journal stated, "Hackers targeted Turkish lender Akbank in a cyber-attack on the SWIFT global money transfer system, the bank said, adding it faced a liability of up to $4 million from the incident but no customer information was compromised".

2017: Taipei Times reported in 2017, "Far Eastern on Friday said it reported to the Financial Supervisory Commission that malware had been implanted in its computer system, which affected some of its PCs and servers, as well as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network". The Focus Taiwan said," Through the planted malware, hackers conducted virtual transactions to move funds totaling nearly US$60 million from Far Eastern Bank customers' accounts to some foreign destinations such as Sri Lanka, Cambodia and the United States, the bank found on Tuesday".

2018: The Habib Bank Limited became a victim of ATM skimming. The Habib Bank Limited confirmed that over Rs10 million had been stolen from 559 of its accounts. Dawn says, "Hundreds of thousands of rupees have been skimmed out of 32 accounts of a private bank located in the Saddar area of Rawalpindi, indicating the presence of ATM hackers in the twin cities including Islamabad". Another report by Dawn says," Several foreigners have been arrested for allegedly stealing data from banks using skimming devices at ATM facilities".

1.10.4. Africa

2016: According to Serianu report, "cyber criminals employed a very complex cybercrimes targeting 10 organizations in banking, insurance, utilities and government across 3 countries in Africa." According to this report damages to banking and financial service sector (as a result of cyber-attack is highest among all sectors) that is $206m in 2016. At least 19 organizations in Kenya have been affected by the ransom ware virus in an on-going global hacking.

1.10.5. Australia

The banking, financial services and insurance sector are clearly one of the most prone industries to cyber-crimes, CBA which became a victim of cyber-crime in 2016.

Hundreds of thousands of Australians have been targeted by a fake Commonwealth Bank email designed to infect recipients with malware. Customers and noncustomers are vulnerable to the scam, which asks people to click to view a 'Secure Message'. Furthermore, those who take the bait will in fact download a trojan used by cybercriminals to hack computers.

1.10.6. Claessens et al., (2002)

There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and credit Card Frauds. However, in general all the frauds are executed with the ultimate goal of gaining access to user s bank account, steal funds and transfer it to some other bank account. In some cases the cyber criminals uses the banking

credentials like PIN, password, certificates, etc. to access accounts and steal meagre amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts.

1.10.7. Beirstaker, Brody, Pacini (2005)

Suggested various techniques such as fraud vulnerability reviews, fraud policies, telephone hotlines, employee reference checks, vendor contract reviews and sanctions, analytical reviews (financial ratio analysis etc.), password protection, firewalls protection, digital analysis and other forms of software tools to detect and control frauds.

1.10.8. Gupta P.K. (2008)

In the study 'Internet Banking in India – Consumer Concerns and Bank Strategies' tried to identifies the weaknesses of conventional banking and explores the consumer awareness, use patterns, satisfaction and preferences for Internet banking vis-a-vis conventional form of banking and also highlighed the factors that may affect the bank's strategy to adopt Internet banking. It also addressed the regulatory and supervisory concerns of Internet banking.

1.10.9. Ashu Khanna, Bindu Arora (2009)

In their survey based work 'A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry' done to find out the attitude of and measures taken by bank employees/ managers in controlling banking cybercrimes observed the bank employees do not give due importance to the problem of frauds. The awareness level of bank employees regarding bank frauds is not very satisfactory, and majority of them do not dispose favourable attitude towards RBI procedures as they find difficulty in following them due to workload and pressure of competition.

1.10.10. Moore.T, Clayton.R&Anderson.R (2009)

Focused on the subject of online crime. Online crimes mostly occur from the nuisance came from amateur hackers. This paper looks at the data of online crime and many problems. Problems that banks and police forces face in controlling the traditional law enforcement. The analysis of this paper show that significant improvements are possible in the way dealing with online fraud and to study the online crime it is suggested that to understand its economic perspective.

1.10.11. Florêncio&Herley, (2011)

As a lot of vulnerabilities exist in the defence system of banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and combat such crimes.

1.10.12. Hemraj Saini, Yerra Shankar Rao & T.C.Panda (2012)

In their study 'Cyber-crimes and their Impacts: A Review' have described the problem and kinds of cybercrimes with their effects on different segments the society in general.

1.10.13. B. Singh (2013)

In their report 'Online Banking Frauds In India' has observed that Cybercrimes in India are on rise thanks to the growing use of information technology. With limited numbers of cyber law firms in India, these cybercrimes are not reported properly. Even the cyber security of India is still catching up with the present requirements.

1.10.14. BBC NEWS (27 March 2015)

Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial affairs on the internet. The rise is due to increased use of computer malware and con-artists tricking consumers out of personal details. Overall losses on UK cards from fraud totaled £479m in 2014, up 6% on 2013, according to Financial Fraud Action. The total amount of fraud is down 21% from the peak of £609.9m in 2008. The figures also showed that losses caused by criminals using UK cards fraudulently abroad, where they can circumvent some security features, were up sharply. Losses increased to £150.3m in 2014, up 23% from the previous year. The figures come in the same week as fraud prevention service Cifas said that 46-year-old men were the most likely victims of identity theft.

1.10.15. Business Standard (2015)

With the increase in banking on mobile phones and the internet, financial frauds in the system have also seen an uptick, says a survey on financial frauds in the financial sector by Assocham and PwC. The report said that financial frauds led to approximately $20 billion (Rs 1.26 lakh crore) in direct losses annually. The report states that currently, 74 per cent of the population has mobile

phones and this has led to a steady rise in banking on the go. According to Reserve Bank of India data, the volume of mobile banking transactions has risen from around Rs 1,819 crore in 2011–12 to approximately Rs 1,01,851 crore in 2014-15. Whether it's financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions.

1.10.16. Business Insider India (2015)

Consulting arm of Mahindra Group, suggests that the number of cybercrimes in the country is expected to double and cross the 3-lakh mark in 2015. As per the study, the cybercrimes are

growing at a rate of 107% year on year while registering over 12,000 cases every month. According to the report, the number of cases of cybercrimes was 13,301 cases in the year 2011, which was followed by 22,060 such cases in 2012 and 71,780 cases in 2013. By May 2014 alone, the cyber cells in India had registered a whopping increase in cybercrime cases and registered 62,189 cases. The increasing use of mobile, smart phones, tablets for online banking and financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age groups, stated the report. The economic growth of any nation and its security whether internal or external and competiveness depends on how well is its Misuse of the ATM-cum-debit card had been a common problem for all. Often debit card users report fraudulent transactions have been made through their ATM cards even when the cards were in their possession.

1.10.17. Worldly post (Karthik,2015)

Assocham-Mahindra SSG study has released a report stating the number of cybercrimes in India may double to 3 lakhs in 2015. India now being the favourite and easy to target for cybercriminals, mostly hackers, other malicious users could pose serious economic and national security challenges. India has been prone for all the identity theft, spamming, phishing and other types of fraud, as there is an upturn usage of Smart phones and tablets for online banking and other financial transactions in recent times. The Study also

revealed that ―the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE are the countries from where most of the cyber space attacks have been originated, which is a major concern. India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014. As per the study, Andhra Pradesh, Karnataka and Maharashtra are in top three positions in 2014 when it comes to the number of cybercrimes cases registered under the new IT Act in India. It further added, these three states together contribute more than 70 percent to India`s revenue from IT and IT related industries.

1.10.18. PTI New Delhi (2015)

The increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. Rising at an alarming rate, the number of cybercrimes in

the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges. India has emerged as a favourite among cybercriminals, mostly hackers and other malicious users who use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud. As per the study's findings, total number of cybercrimes registered during 2011, 2012, 2013 and 2014 stood at 13,301, 22,060, 71,780 and 1, 49,254 respectively. The origin of these crimes is widely based abroad in countries like China, Pakistan, Bangladesh and Algeria, among others. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. Maximum number of offenders belong to the 18-30 age group, added the report. The study revealed that the attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE. It further stated that mobile frauds are an area of concern for companies as 35-40 per cent of financial transactions are done via mobile devices and this number is expected to grow to 55-60 per cent by 2015.Rising Internet penetration and online banking have made India a favourite among cybercriminals, who target online financial transactions using malicious software (malware). India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014, the study said. Andhra Pradesh, Karnataka and Maharashtra have seen the highest number of cybercrimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries.

1.10.19. Tewari R.K, Sastry P.K and Ravikumar K.V.

In their book "Computer Crime and Computer Forensics" the author describes the Computer Networking and the Internet. He further discussed the Vulnerabilities of Computer Networks. The author described the emergence of Computer Crime and the Internet Crimes and Network Security Measures. He commended on Digital Signatures and Cryptography. He discussed the National and Int6ernational coordination to handle the cybercrime.[1]

---

1. Tewari R.K, Sastry P.K and Ravikumar K.V "Computer Crime and Computer Forensics" Select Publishers Delhi 2002

1.10.20. M.I.Tannan

in his book "Banking Law & Practices," the author gives the every details knowledge about the banking laws & practices in India. It has covered every aspect and every law prevalent for Banking Regulation in India, the book reflects the early history of the banking in India[2.]

1.10.21. Hogson, N. F

In his book "Banking through the Ages," the author describes the early banking system in the various parts of India.[3]

1.10.23. S.B.Verma, S.K.Gupta & M.K.Sharma

In their book "E-Banking and Development of Banks" described the general history of banking. The Authors further described the adoption of IT in banking has undergone several changes with the passage of time. Today IT has become an inseparable segment of banking organization. The application of information technology in the banking sector resulted in the development of different concepts of banking such as – E-banking, Internet Banking, Online Banking, Telephone Banking, Automated teller machine, universal banking and investment banking etc.[4]

1.10.24. Nandan Kamath

In his book "Law relating to computers, Internet and E-Commerce (A guide to Cyber Laws and the Information Technology Act, 2000)," the author commented on the cyberspace as it

---

2. Tannan M.L "Banking Law and Practice in India", 28th edition, India Law House Connaught Place, New Delhi.
3. Hogson, N. F. Banking Through the Ages, (1926) New York, Dodd, Mead & Company
4. Verma S.B., Gupta S.K. and Sharma M.K.," E-Banking & Development of Banks", Deep & Deep Publications Pvt.Ltd. Delhi 2007

becomes a money spinner and it will increasingly become the domain of business legal & illegal. As a potential information technology power, India should take warning from the hunting hackers and put the legal system on guard. The author also discussed the importance of electronic evidence in the case of cybercrimes. He further added about the legitimacy of the electronic records to be produced as electronic evidence. He exhaustively explained about the burden of proof related to electronic evidence. [5]

1.10.25. R.C.Dutt

In his book "Civilization in Ancient India," the author in his book described in detailed about the banking in ancient India. [6]

1.10.26. Buhler

In his book "The laws of Manu, the Sacred Books of the East," the author in his book discussed in detailed the provisions of punishment as per "Manusmriti". [7]

1.10.27. Rupa Mehta and Rohinton Mehta

In their book "Credit Cards a Legal Guide" with special reference to Credit Card Frauds, the authors described the proliferation of credit cards in our daily lives and the billion dollars of fraud perpetrated using credits. The authors commented on Money and Plastic Money, Types of Cards, Smart Cards and features of Cards. He explained the Card Cycle. They further discussed Credit Card Fraud and Fraud detection techniques. They explained Credit Card Fraud Investigation techniques. The authors further commented on Credit Cards and Criminal Law and the Liability of Banks & Card holder. [8]

---

5. 0 Kamath Nandan, "Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000", Universal Law Publishing Co., 2009
6. Dutt R.C.,"Civilization in Ancient India " Vol.1, revised edition.
7. Buhler, "The laws of Manu, the Sacred Books of the East" ,Vol.XXV,p.286
8. Mehta Rupa and Mehta Rohinton "Credit Cards a Legal Guide" with special reference to Credit Card Frauds, Universal Law Publishing Co.Pvt.Ltd Delhi Second Edition 2009.

1.10.28. Austin, Granville

In his book ”Working a Democratic Constitution – A History of the Indian Experience”, described the prevailing economical financial situation before the nationalizations and how Indira Gandhi the then prime minister had taken the decision of nationalization of 14 big banks under the control of private management to boost the perception of social control. [9]

1.10.29. Justice Yatindra Singh

In his book “Cyber Laws” has described the adoption of IT in banking has undergone several changes with the passage of time. The application of information technology in the banking sector resulted in the development of different concepts of banking such as – E-banking, Internet Banking, Online Banking, Telephone Banking, Automated teller machine, universal banking and investment banking etc. Information technology has a lot of influence on banking transactions. He further threw light on trademarks, copyrights, patents & their existence in cyber space. [10]

1.10.30. Toor, N.S

In his book “Handbook of Banking Information”, the author described that the automation in the banking sector has come a long way starting with the Rangarajan Committee report on the banking sector reforms during the eighties, followed by reports of the Narasimham Committee in the nineties. He threw light on the core banking solutions (CBS,) RBI guidelines on Universal Banking, Clearing Corporation of India Ltd. (CCIL) and Anti Money Laundering Act, 2002. [11]

1.10.31. Manikyam K.Sita Mrs. Dr.

In her book “Cyber Crimes” Law & policy perspectives” described the basic concepts of

---

9. Granville Austin,”Working a Democratic Constitution – A History of the Indian Experience”. New Delhi: Oxford University Press1999
10. Singh Yatindra Justice, Cyber Laws, Universal Law Publishing Co. Pvt. Ltd. 2010
11. Toor, N. Handbook of Banking Information,Skylark Publications, 28th edition 2009

cyber space like meaning, types, features and major components of computers; history and development of internet; merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. She highlighted the importance of computers and internet in day-to-day jobs. She further expressed that cyber-crimes touches and influences almost every aspect of daily routine of each one. We are in the information age and dependent on computers as those are the source of inspiration. She threw light on the Information Technology Act 2000 and Information Amendment Act 2008. She also pointed out the loop holes. She also described the comparative study of cyber laws of the different countries. [12]

1.10.32. N. C. Jain

In his book "Cyber Crimes," the author discussed about the technology based cybercrimes like Viruses and worms. He explained the various varieties of virus like Stealth virus, Polymorphic Virus, Sparse infector a virus that infects the computers only occasionally, Companion virus that creates a new programme by doing modification in an existing files, Armored virus, Macro virus, Virus hoax. He also explained the worms which uses a network to spread functional copies of it to other computer systems. He also described the "Trojan Horse" which is a program that locates password information or makes the system more vulnerable to future entry or may simply destroy programs or data on the hard disk. He also described about Website Compromise and Malware Propagation. He also described the various malwares like Adware, Bots, Bugs, Ransomware, Rootkits and Spyware. [13]

1.10.33. Sinha, S. L. N.

History of the Reserve Bank of India, the author in his book described the history and formation of the Reserve Bank of India. [14]

---

12. Manikyam K.Sita Mrs.. Cyber Crimes" Law & policy perspectives 2009 edition ,Hind Law House Pune
13. Jain N.C " Cyber Crimes" Allahabad Law Agency, Delhi 2008
14. Sinha,S. L. N. History of the Reserve Bank of India, Volume 1: 1935–1951. RBI. 1970

1.10.34. Baibridge D.

In his book "Introduction to Computer Law", the author described the cyber frauds, its definition and types of the cyber frauds. He also described the ATM frauds and Card Trapping Attack. Skimming Attack, Phishing/Vishing Attack, Pin Cracking Attack, ATM Hacking. ATM Malware Attacks, Carders, the people who buy, sell, and trade online the credit card and Internet Search Engine/Google "Hacking". [15]

1.10.35. Vivek Sood

In his book "Cyber Crimes, Electronic Evidence and Investigation Legal Issues" has described the nature and types of cybercrimes and recommended various methods to control cybercrimes. He further described the electronics evidence in the court and its critical analysis and stepwise process; He also explained the electronic evidence and criminal investigations. He critically analysis the burning problem that why India should sign the convention on cybercrime and why it is essential He concluded that cyber and computer related crimes cannot be fought on a standalone basis and nations must come together to combat these crimes and for collection of electronic evidence with respect other crimes. [16]

1.10.36. Vivek Sood,

In his book "Cyber Law Simplified" the author criticized the Power of Arrest without Warrant under the IT Act, 2000.He threw light on Cyber Crime and Criminal Justice, He also discussed Penalties, Adjudication and Appeals under the IT Act 2000. He discussed the Contracts in the Cyber World and Jurisdiction in the Cyber World. In this book he also discussed Battling Cyber Squatters and Copy right Protection in the Cyber World. He critically analyzed Digital Signature, Certifying Authorities and E-Commerce. He further discussed the Indian Evidence Act of 1872 and Information Technology Act 2000. [17]

---

15. Baibridge D., Introduction to Computer Law, 4th Ed. 2000
16. Sood Vivek , Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 2010
17. Sood Vivek "Cyber Law Simplified" Tata Mc Graw-Hill Publishing Company Limited, New Delhi 2003

1.10.37. Ahemad Farooq Dr

In his book "Cyber Law in India"(Law of Internet), the author described the Development of computers and Internet. He further described the potential and problems of the Internet. He discussed the Genesis, Objects and Scope of the IT Act. He threw light on Encryption, Authentication of Electronic Records and Electronic Governance. He described the Certifying Authorities, Domain Name Disputes and Trademark Law, Electronic Commerce and service Providers Liability for Copyright Infringement. He also explains the Cyber Appellate Tribunal. He also described the classification of Cyber Crimes. [18]

1.10.38. Harish Chander

In his book "Cyber Laws and IT Protection", the author described the International Efforts relating to Cyber space Laws and Cyber Crimes. He further described the council of Europe Convention on Cyber Crime, He commented on the Penalties, Compensation and adjudication of violations of provisions of IT and Judicial review. In his book the author described the role of Electronic Evidence and miscellaneous provisions of the IT Act. [19]

1.10.39. Jonathan Rosenoer

In his book "Cyber Law: The Law of the Internet" the author discussed the Copyright and Trade Mark in the Cyber Space. He further discussed the defamation and privacy issues and criminal liability. The author commented on Electronic Contracts and Digital Signature. The author further commented on Ecommerce and cyber laws. He further commented on misappropriation of Information and Evidence. [20]

---

18. Ahemad Farooq Dr. in his book "Cyber Law in India"(Law of Internet) published on Pioneer Books Delhi,
19. Harish Chander "Cyber Laws and IT Protection" published by PHI Learning Private Limited New Delhi,2012
20. Jonathan Rosenoer, "Cyber Law: The Law of the Internet published by "Springer"1996

1.10.40. Russell G.Smith

Peter Grabosky and Gergor Urbas, in their books "Cyber Criminals on Trail" the authors defined the cybercrimes and measured the cybercrimes. Further they discussed how the prosecutors are acted as gate keeper of Cyber Crimes. The authors commented on the cross border issues and strategies of Cyber Crime Legislation. They discussed in the book the quest for harmonization of Cyber Crime Law and judicial punishment in cyber space. At the last they described the sentencing Cyber Criminals. [21]

1.10.41. ARTICLES

1.10.41.1. Bhagvati R. Pipaliya

In his article "An Empirical study on Consumer Awareness on Internet Banking in Gujarat" discussed the e-banking and the popular services including Automated Teller Machines, Credit Cards, Debit Cards, Smart Cards, Electronic Funds Transfer (EFT) System and Cheque Truncation Payment System and Mobile Banking. He further discussed the advantages of e-banking. The main advantages are the operating cost per unit services is lower for the banks. It offers convenience to customers as they are not required to go to the bank's premises. There is very low incidence of errors. The customer can obtain funds at any time from ATM machines. The credit cards and debit cards enables the Customers to obtain discounts from retail outlets. The customer can easily transfer the funds from one place to another place electronically. [22]

1.10.41.2. Shamsul Haq and Bilal Mustafa Khan

In their article 1 "E-Banking Challenges and opportunities in The Indian Banking Sector"

---

21. 6 Russell G.Smith, Peter Grabosky and Gergor Urbas, " Cyber Criminals on Trail" published by Cambridge University Press,2004
22. Pipliya Bhagwati R,"An Empirical study on Consumer Awareness on Internet Banking in Gujarat" published in edu.philica.com

commented that banks could be able to reduce the rush at the branches and operating cost also therefore .Banks are now spending heavily on information technology front but from the side of the government there is requirement to invest on the infrastructure like electricity and internet. It is useful from the view of clients as well as the banks therefore in the coming years Ebanking reshape the traditional banking.

1.10.41.3. R. K. Uppal

In his article "Internet banking in India: Emerging risks and new Dimensions" highlighted the benefits of i-banking to customers as well as to bankers and suggests some strategies with their possible solutions like to spread awareness regarding I-banking and to increase its area and scope to enhance I-banking services in India, particularly in rural and semi-urban areas.[23]

1.10.41.4. Jyotiranjan Hota

In his article "Growth of ATM Industry in India" concluded as Though, ATM industry is growing rapidly, there are many challenges related to security issues of the software, increase of rental costs by the day in major cities, housekeeping, and replenishment of cash. Few banks have introduced biometric ATMs in rural India, which are quite secure and easy to use by a common man. Banks are trying to shift slowly from multi-vendor to multi-channel integration, so as to get a complete picture of the activities of customers. [24]

1.10.41.5. Behra, Abhimanyu

In his article "Cyber Crime and Law in India", has classified the various types of cybercrimes on the basis of nature and purpose of the offence committed. It can be broadly grouped in three categories based on the target of the crimes, a) where computer is the target of crime. b)

---

23. Uppal R.K."Internet banking in India: Emerging Risks and New Dimensions" published in Prime Journal, Business Administration and Management (BAM) Vol. 1(3), March 10th 2011.
24. Hota J."Growth of ATM Industry in India" published in CSI Communications February 2013.

Where computer facilitate commission of crime. c) Where computer is incidental to the crime and also suggested strategies to control the cybercrime. The major suggestions are a) The Act should be amended suitably in consonance with the development of Science and Technology, b) Cyber cells shall be formed in all the police station throughout the country. Net policing is the need of the hour. c) Judges and police officers and lawyers must be given appropriate training about cyber laws and its enforcement.

1.10.41.6. Mittal R. K. and Dhingra Sanjay

in their article that transaction through technology channels cost much less to the banks than the customers reaching the bank and doing the transactions. In the last decade banks have invested heavily in the technology. In the use of information technology, the new private and foreign sector banks have taken lead over the public and old private sector banks. Today public sector banks are investing heavily in technology to compete with the new private and foreign sector banks.[25]

1.10.41.7. Radhakrishna Geeta and Pointon Leo

In their article "Fraud in Internet Banking: A Malaysian Legal Perspective", commented that the paper examines the legal issues specific to internet banking, focusing on the incidence of fraud and its prosecution. The objective of research is to investigate three questions in relation to Malaysia. Firstly, the incidence of fraud in internet banking; secondly, the adequacy of the relevant regulations and statutes; and thirdly, whether the setting up of a cyber-court would better facilitate the prosecution of such financial crimes in Malaysia. Technology and the borderless nature of the internet present fraudsters with manifold opportunities. 'Phishing' leads to identity theft and 'money laundering' has been found to be the main threat to internet banking, the selected fraud for study in this paper. [26]

---

25. Mittal R.K. & Dhigra S. "Technology in Banking Sector: Issues and Challenges", Vinimay,Vol.XXVII, No.4, 2006-07
26. Radhakrishna Geeta and and Pointon Leo, "Fraud in Internet Banking: A Malaysian Legal Perspective", ICFAI University Journal of Bank Management, Vol. VI, issue 1 (Feb. 2007), pages 47-62

1.10.41.8. Rahul Goel

In his article "The Indian Information Technology Act and Spamming" pointed out that as per International Telecommunication Union (ITU), "although there is no a single solution to overcoming spam, appropriate legislation and effective enforcement are two of the main elements in the fight to combat the problem. As the phenomenon of spam is relatively recent, not all countries have spam laws, and even those that have already implemented specific legislation are currently facing the problem of enforcement at the national and international level. Furthermore, spammers (often also scammers) are increasingly exploiting the international nature of the Internet. For this reason, cross-border cooperation is crucial both in the elaboration and the implementation of new legislation and in its subsequent enforcement.[27]

1.10.41.9. Hebbar Raveendranath

In his article "Building trust in E-Banking", described that Managing Technology is a key challenge for the Indian Banking Sector. Banks have enhanced their network and communication infrastructure to reap the full benefits of computerization. E-banking is catching up. The need for having required tools for trust, privacy and confidentiality is a major area of concern for today's network banking. Public Key Infrastructure (PKI) provides the frame work of trust essential for e-business to strive.PKI system are used to generate & verify Digital Signature, which can be attached to messages for imparting necessary authenticity integrity and non-repudiation policies, procedure and systems are being laid out by RBI and the Structural Financial Messaging Systems (SFMS) being introduced in bank under the aegis of IDBRT is expected to revolutionize the way banking is conducted in the country. The Real Time Gross settlement (RTGS) system being introduced in the country is built the trust level guaranteed by the SFMS backbone.[28]

---

27. Goel Rahul, "The Indian Information Technology Act and Spamming" Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1
28. Hebbar Ravindranath "Building trust in E-Banking", Vinimay, Vol. XXIV. No 4, 2003-04

1.10.41.10. Shreyan Singh, Sohrab Singh Chattwal, Taha Mohammed Yahyabhoy and Yeo Chin Heng

In their article "Dynamics of Innovation In E-Banking" concluded as By applying the Revised Technology Life Cycle to two discontinuous e-banking innovations – ATMs and Internet Banking, we have established that the Life Cycle provides a useful outline for successful strategies that can be adopted by banks and other financial institutions as technology evolves.[29]

29. Shreyan Singh, Sohrab Singh Chhatwal, Taha Mohammed Yahyabhoy and Yeo Chin Heng in their article "Dynamics of Innovation In E-Banking"

CHAPTER – II

RESEARCH METHODOLOGY

CHAPTER – II

RESEARCH METHODOLOGY

2.1. Research Methodology

It is an explanatory research and uses qualitative approach to elaborate the impact of cybercrime in banking sector. Review of literature provides the base about the concept but effect is still unclear. Therefore mixed (hybrid) method is adopted. This is global study on cybercrime in banking sector.

This study is based on descriptive method on secondary data to fulfil the object of the study the category of cybercrime has been analysed by reviewing the various literature book and studies. The researcher has visited the various web sites and goes through the information related to subject. Similarly various group and e-book were visited on the web-site and collected the related data for the study. The comprehensive list of the websites is given in the bibliography.

Some national newspapers as well as local newspaper were gone through for the news related to cybercrime as well as cyber laws, the list of such newspapers is given in the bibliography.

The various law magazine as well as the other magazines like IBA bulletin, RBI bulletin, and various National and International Journals were read for information related to cybercrime as well as cyber laws. The necessary information was jotted down and used in the study. The list of such magazines and journals is given in the bibliography.

For the study of tricks and techniques use by the cyber criminals to hack the banking system and make the cyber frauds, various case studies in various news channels referred. Further, research objectives data gathered from annual reports of national crime record bureau (NCRB).

Examine the growth of cybercrime incidents and for drawing inferences following data has been chosen:

1) Indian Computer Emergency Response Team – India (CERT-In) is a functional organization of Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. The Information Technology Act, 2000 by virtue of Section 70 A and Section B designated CERT-In to serve as the national agency to perform the functions of collection, analysis and dissemination of information on cyber incidents in the area of cyber security. CERT-In has started publication of data since 2004 on the various cybercrime incidents. The cybercrime incidents related to banking published by CERT-In taken as under:

1. Phishing,
2. Network Scanning/Probing,
3. Spreading Virus/Malicious Code,
4. Spam,
5. Website Compromise and Malware Propagation and
6. Other Incidents.
7. Total Cyber security

The total of these cyber incidents is also taken into consideration. For the purpose of Statistical Analysis and drawing inferences a period of 7 years has been chosen commencing from 2009 to 2015.

2) Reserve Bank of India published data of Cyber Crime incidents of fraud in Scheduled Commercial Banks in India every year since 2008-09. For the purpose of Statistical Analysis and drawing inferences a period of 7 years has been chosen commencing from 2008-09 to 2014-15.

Data of Cyber Crime fraud Incidents taken from Commercial Banks in India as under:

***List of Schedule Commercial Bank of India**

COMMERCIAL BANKS IN INDIA					
S.N.	PUBLIC SECTOR BANKS	S.N	PRIVATE SECTOR BANKS	S.N.	FOREIGN BANKS
	(A) NATIONALISED BANKS				
1.	Allahabad Bank	1.	Axis Bank Ltd.	1.	American Express Banking Corporation
2.	Andhra Bank	2.	Development Credit Bank	2.	Barclays Bank PLC
3.	Bank of Baroda	3.	Dhanlaxmi Bank Ltd.	3.	Citi Bank N.A.
4.	Bank of India	4.	Federal Bank Limited	4.	Deutche Bank (Asia)
5.	Bank of Maharashtra	5.	HDFC Bank Ltd.	5	Firstrand Bank
6.	Canara Bank	6.	ICICI Bank Ltd.	6.	Hongkong & Shanghai Banking Corp. Ltd
7.	Central Bank of India	7.	Bank of Rajasthan Ltd. (Merged With ICICI)	7.	Standard Chartered Bank
8.	Corporation Bank	8.	IndsInd Bank Ltd.		
9.	Dena Bank	9.	Jammu & Kashmir Bank		
10.	IDBI Bank Limited	10.	Karur Vysya Bank Ltd		
11.	Indian Bank	11.	Kotak Mahindra Bank Ltd.		
12.	Indian Overseas Bank	12.	Laxmi Vilas Bank Ltd		
13.	Oriental Bank of Comm.	13.	South Indian Bank Ltd.		
14.	Punjab National Bank	14.	Tamilnad Mercantile Bank		
15.	Syndicate Bank	15.	The Royal Bank Of Scotland		
16.	UCO Bank				
17.	Union Bank of India				
18.	United Bank of India				
19.	Vijaya Bank				
	(B) STATE BANK GROUP				
1.	State Bank of India				
2.	State Bank of Bikaner &Jaipur				
3.	State Bank of Hyderabad				
4.	State Bank of Indore (Merged with SBI)				
5.	State Bank of Mysore				
6.	State Bank of Patiala				
7.	State Bank of Travancore				
(i)PUBLIC SECTOR BANKS=26		(ii)PRIVATE SECTOR BANKS=15		(iii)FOREIGN BANKS=7	
TOTAL COMMERCIAL BANKS (I+II+III)=48					

3) The Minister of State for Finance, Shri Namo Naraian Meena in a written reply to a question in the Lok Sabha on 22nd February 2013 replied that the details furnished by Reserve Bank of India (RBI) in respect of Scheduled Commercial Banks pertaining to frauds relating to ATMs/Debit Cards/ Internet Banking and Credit Cards for the last four calendar years i.e. 2009 to 2015. Researcher has chosen the data for the Public Sector Banks for the 7 calendar years i.e. from 2009 to 2015 for the purpose of Statistical Analysis and drawing inferences. List of public sector banks is given in the above table.

Population

- All the banks whether national or international is the population of the study.
- Data collection from secondary source because of limited time and budget. The secondary source includes Books, E-Source, Journals, Articles and Newspapers.

Tool Used

Because of secondary data is chosen no other tool was used. The research relied on the secondary data such as books journals, e-sources, articles and newspapers.

Limitation of the Study

1. Researcher had to rely on secondary source available in books and e-sources to gather information about the study.
2. The scope of study is limited to the banking sector only.

CHAPTER – III

CONCEPT OF CYBER CRIME IN BANKING SECTOR

CHAPTER – III

CONCEPT OF CYBER CRIME IN BANKING SECTOR

3.1. Cyber Crime

Cybercrime or computer oriented crime is a crime that involves a computer and a network. The computer may have been used in the common of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly and indirectly, using modern telecommunication network such as Internet (networks including but not limited to Chat rooms, e-mails, notice board and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrimes may threaten a person or a nation's security and financial health. Issues surroundings these types of crimes have become high-profile, particularly those surroundings hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Further cybercrime from the perspective of gender and define 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".

3.2. Evolution of Cyber Crime

During the period of 1950's, it would be an astonished feeling for everyone who uses palmtops and microchips today, to know that the first successful computer was built and the size of the computer was so big that it takes the space of entire room and they were too expensive to operate. The functioning of these computer were not understandable to large number of people and only select people with expertise had direct access to such computers, and has the knowledge to operate them. For obvious reasons, the computer technology was extremely expensive and

beyond the purchasing capacity of almost the entire population until IBM's came into being wherein it introduced its stand-alone "personal computer" in 1981 and exposing many to the rewards of quick data access and manipulation that, up to that time, had been realized by few. The Personal computers become cheaper and become household item at the start of 21st century in India. The Internet was first started by the US department of defence, after World War II with the idea to have a network which could work in the event of disaster or war and securely transmit information. The First Network was known as ARPANET, with the development of Transmission Control Protocol/Internet Protocol, World Wide Web and Hypertext the internet become rage all over the world. With the growth of Internet the quality and variety of information grew. However at that point nobody anticipated the opportunities' the internet is going to provide the technology savvy criminals.

In India the internet services started by the state-owned Videsh Sanchar Nigam Limited in year 1995 and in 1998 the government has ended the monopoly of VSNL and market is opened to private operators. At that point, the internet users in India are 0.1% of total population, and now India has become the 2nd largest country in terms of internet users after china with 33.22% people using internet.[30]

The process of criminalization of human behaviour judged to be harmful the public is typically one that builds slowly in common law jurisdictions. Momentum gained through problem identification and pressures exerted mg special interest groups can easily span decades before undesirable actions are classified as "crime". In some instances, this process is accelerated through the occurrence of certain "catalyst events" that capture attention of the public and the attention of lawmakers.[31]

The first recorded cybercrime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modem computers, however, began with the

---

30. https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users (Accessed on 3rd February, 2016)
31. Abraham D. Sofaer, Seymour E, .The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, 2001.

analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cybercrime.[32]

In the case of computer crime, legislators grew increasingly attentive is the 1980's as business became more dependent upon computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations. Criminals can now easily encrypt information representing evidence of their criminal acts, store the information and even transmit it with little fear of detection by law enforcement. Due to the extraordinary impact of the Internet, a computer crime scene can now span from the geographical point of the victimization (e.g., the victim's personal computer) to any other point on the planet, further complicating criminal investigative efforts. In effect, computer technology has dramatically altered the criminal justice terrain such that enterprising and opportunistic criminals have consciously turned to the computer to commit their illegal acts in situations in which the computer serves as the instrument of the crime, the means by which the crime is committed, as well as in cases in which the victim's computer, or computer system, is the target, or objective, of the act. And, as stated above, the presence of new computer technology aids cyber criminals in situations in which the computer's role is incidental to the crime; situations in which the computer is used to house and protect information that is evidence tying the offender to criminal acts. A commonality among these types of crimes is that the offender, to a great degree, depends upon the lack of technological skills of law enforcement to successfully commit the offenses and escape undetected. Based upon what empirical evidence has been available on self-assessed skills of investigators in this area, computer criminals would have good reason to feel some confidence in their chances to evade detection of their crimes.[33]

---

32. http://cybercrime.planetindia.net/intro.htm (Accessed on 4th February, 2016)
33. Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Report, Washington, Dc: U.S. Department of Justice, March 2001.Available at : https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf (Accessed at 04th February, 2016)

As we advance towards the 21st century, it van be observed that the technological innovations have laid the way for the entire population using computer technology today, to experience new and wonderful conveniences in their daily life ranging from how to educated, shop, entertain, to availing the understanding of the business strategies and work flow. Our day to-day lives have been forever changed thanks to rapid advances made in the field of computer technology. These changes allow us to communicate over great distances in an instant and permit us, almost effortlessly, to gather and organize large amounts of information, tasks that could, otherwise, prove unwieldy and expensive. The technological treasures that have improved the quality of our lives, however, can reasonably be viewed as a doubled-edged sword. While computer technology has opened doors to enhanced conveniences for many, this same technology has also opened new doors for criminals.

3.3. Cyber Crime in Banking Sector

Economy is one of the pillars which defines the progress and growth of a nation. Banking sector is considered as the backbone of the economy. For our day-to-day transactions, we enter into monetary transactions in the form of cash payments, cheques or demand drafts. However, this trend has paved the way to a modern system of payment in the form of swiping of debit cards or credit cards.

On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998, information and technology in banking sector was used. On one hand, technology has created advantage for banks and financial institutions but on the other hand, there have been risks involved in it as well. Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information.

Banking sector has witnessed expansion of its services and strives to provide better customer facility through technology but cyber-crime remains an issue. Information which is

available online is highly susceptible to be attacked by cyber criminals. Cyber-crimes result in huge monetary losses which are incurred not only by the customer but by the banks also which affects economy of a nation. Non-monetary cyber-crime occurs when viruses are created and distributed on other computers or confidential business information is posted on Internet. The most common of it is phishing and pharming.

3.3.1. Concept of E-Banking

Electronic Banking or e-banking refers to a system where banking activities are carried out using informational and computer technology over human resource. In comparison to traditional banking services, in e-banking there is no physical interaction between the bank and the customers. E-banking is the delivery of bank's information and services by banks to customers via different delivery platforms that can be used with different terminal devices such as personal computer and a mobile phone with browser or desktop software, telephone or digital television.

The first initiative in the area of bank computerization was stemmed out of two successive Committees on Computerization (Rangarajan Committee). The first committee was set up in 1984 which drew the blueprint for the mechanization and computerization in banking industry. The second Committee was set up in 1989 which paved the way for integrated use of telecommunications and computers for applying fully the technological breakthroughs to the banking operations. The focus shifted from the use of Advanced Ledger Posting Machines (ALPMs) for limited computerization to full computerization at branches and to integration of the branches. Till 1989, banks in India had 4776 ALPMs at the branch level, over 2000 programmers/ systems personnel and over 12000 Data Entry Terminal Operators. E-banking is also known as Cyber Banking, Home Banking and Virtual Banking. E-banking includes Internet Banking, Mobile Banking, RTGS, ATMs, Credit Cards, Debit Cards, and Smart Cards etc. Some of the forms of E-banking are explained below:

3.3.1.1.Automated Teller Machines (ATMs)

An ATM is a device which is located on or off the bank‟s premises. It enables a customer to withdraw cash, obtain statement of last few transactions in his/her account, deposit cash and

to transfer funds from one account to another. A person can withdraw cash 24x7 from ATMs subject to the limit provided. This system is also known as „Any Time Money" or „Anywhere Money". To have access of ATM a person must have an ATM card.

The ATM card is inserted into the machine and the client is required to enter a personal identification number (PIN). PIN is the numeric password which is separately mailed or handed over or sent by post to the customer by the bank while issuing the card. Most of the banks require that customers change their PIN after first use. Banks also send alerts to the customers not to disclose their PIN to anybody, including to bank officials. Customers should change the PIN at regular intervals. The transactions carried out using ATM machines are quite easy.

There are two types of ATMs, one, exterior ATMs which are located in shopping centers, railway stations, airports etc. and second, interior ATMs which are located within the bank premises. The limits on cash withdrawal at ATMs and for purchase of goods and services are decided by the issuer bank. Nowadays a customer can use ATM of another bank also to withdraw cash. However, in case of such withdrawal at other bank"s ATM, there is a limit of cash withdrawal. Real Time Gross Settlement System (RTGS) RTGS is a system where funds are transferred from one bank to another on „real time" and on „gross basis". RTGS transactions are carried through either interbank or it can be between customers through bank accounts. 'Real Time' means the processing of instructions at the time they are received rather than at some later time; 'Gross Settlement' means the settlement of funds transfer instructions occurs individually (on an instruction by instruction basis). The transactions are settled individually in RTGS.

RTGS transactions are processed throughout the business hours of banks. The timings of business hours at different bank branches are decided by the banks on their own terms and policies. Generally RTGS transactions for customers are available from 9:00 hours to 16:30 hours on weekdays and from 9:00 to 14:00 hours on Saturdays where settlement is to be done at the RBI end. In the RTGS system, mainly large value transactions are processed. The minimum amount that can be remitted through RTGS is Rs. 2 Lakhs. Only minimum limit is provided for payment transaction through RBI settlement. No maximum limit is prescribed for RTGS transactions.

3.3.1.2. Credit Card and Debit Card

Banks issue debit cards that are linked to a customer's bank account. Debit Cards can be used to transfer funds only for domestic purposes from one person to another person. At present, a customer can use his Debit Card to withdraw money, know the monthly statement etc by using another bank‟s ATM, not being the ATM of the bank which issued such debit card. In case a customer transacts through an ATM of another bank from his savings bank account using his debit card then he is not charged by his/her bank upto five transactions which includes both non-financial & financial transactions in a month. However, this five free transaction limit for transactions done at ATM of another bank is restricted to three transactions in six metro cities which includes, Delhi, Mumbai, Chennai, Bengaluru, Kolkata and Hyderabad.

Like Debit cards, it is the banks/other entities permitted by RBI who issue credit cards to a customer. A Credit card has dimension of about 8.5 cm by 5.5 cm. It is a small rectangular shape plastic card bearing the name of the holder of the card i.e., the customer and the account number is printed over it. In addition, the date up to which the card is valid will also be embossed and a specimen signature panel on the revere. A card holder is also given the list of shops and establishments in each city where the card will be accepted in lieu of cash. The limit up to which the card holder can make purchases in a month is also informed to the card holder, this limit is called card limit.

3.3.1.3. Internet Banking

Internet Banking is a result of computerization of banking sector. It was necessary for the banks to open up internet banking activities because of cut-throat competition. Furthermore, Internet banking facility being available at all time has created an advantage for the customers. There has been a paradigm shift from „bricks and mortar‟ to „click and mortar‟ in the banking sector. The first bank to start with internet banking facility was ICICI followed by IndusInd Bank and HDFC Bank respectively in 1999. Internet Banking is beneficial because it is convenient and easy to do banking business from home or at office desk. One can avoid standing in long queues or delays.

Simply by logging using User ID and Password one can experience Internet Banking. With a click on the internet, a customer can check his account statement, transfer funds from one account to another, open FD (fixed deposit), pay electricity or telephone bills or pay rent, can recharge his/her postpaid or prepaid bills etc.

3.3.1.4. Mobile Banking

The importance of mobile phones for providing banking services has increased. We have become dependent on our mobile phones these days. Because of the growth of mobile phone subscribers in India, banking services have been extended for the customers to be availed through their mobile phones. Mobile banking is when transactions are carried out using a mobile phone by the customers that involve credit or debit to their accounts. In 2014, RBI had set up a Committee on Mobile Banking under the Chairmanship of B. Sambamurthy. The Committee is required to study the problems faced by the banks in providing mobile banking to the customers and to examine the options including the feasibility using encrypted SMS-based funds transfer.

Mobile banking facility has witnessed tremendous growth in our country. In the financial year (2016-2017), mobile wallets overtook mobile banking in number of transactions. Mobile wallets transactions; from phone recharges to paying for cabs or shopping online; trebled to almost 400 million through April-November 2016. Mobile wallet system is there in Apps like Jugnoo, Ola, Uber, Mobikwik, Paytm etc.

It has been reported by Times of India that the number of transactions in mobile banking has more than doubled from 98 million to 265 million in the first eight months in the fiscal year of 2016-2017. If the growth continues at such a rate then it is clear that mobile based transactions; be it mobile wallet or mobile-banking transaction, will surpass cheque payment system in some months only. In the present scenario, mobile based transactions added up to 602 million i.e., 83% of the 723 million cheques cleared during April, 2015 to November, 2015. However, the proportion of m-banking was less than 30% till last year. Approximately Rs. 1.26 lakh crore was spent by a customer in 2015 through mobile payments that resulted in a growth of 87% in mobile payment volumes.

If we look at the rise of E-banking it is clear that people have started using this facility more in comparison to the traditional form of banking as evident from the table below for transaction in April-November, 2016 (in millions).

	2015-2016	2016-2017
Cheques	793.1	**729.3**
Online payment RTGS	59.3	**64.0**
Retail Electronic Clearing	890.4	**1922.3**
Mobile Wallets	133.9	**399.1**
Mobile Banking	**97.7**	**203.1**

*Source RBI Payment System Indicator

3.4. Cyber Crime: Types and Its Impact on Banking Sector

Neither crime nor cyber-crime has been defined in IPC or Information Technology Act, 2000 (hereinafter referred as IT Act), but only provides punishment for certain offences. The word „cyber" is synonymous with computer, computer systems and computer network. Thus, it can be said that cyber-crime occurs when any illegal activity is committed using a computer or computer resource or computer network. Douglas and Loader have defined cyber-crime as a computer mediated activity which is conducted through global electronic networks that are either considered illicit or illegal by certain parties.25 Cybercrimes have been classified into four categories by Wall. They are cyber-deceptions, cyber-violence, cyber-pornography and cyber-trespass.26 The frauds in e-banking sector are covered under cyber-deception. Cyber-deception is further defined as an immoral activity which includes theft, credit card fraud, and intellectual property violations. Mostly frauds are committed because of two goals, one, to gain access to the user's account and steal his/her personal information and transfer funds from one account to another. Second is to undermine the image of the bank and block the bank server so that the customer is unable to access his/her account.

In terms of number of cybercrime incidents in ransom ware, an identity theft and phishing attack, India has been ranked among the top 5 countries. According to Global Economic Crime Survey 2014, conducted by PwC, cybercrime was one of the top economic crimes which were reported by various organizations across the world, including India. National Crime Records

Bureau (NCRB) reported that a total of 5,752 persons were arrested for committing cybercrimes during 2014 as compared to 3,301 persons arrested in 2013 registering 74.3% increase over the previous year. Uttar Pradesh (1,223) was reported with the maximum number of persons arrested under such crimes.

Banking sector too has suffered an impact of cybercrimes. RBI has defined bank fraud has as, 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.

`3.5. Cyber Crimes Related With Banking Sector Hacking

Hacking is a crime, which means an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers. The Hacking is not defined in the amended IT Act, 200032. But under Section 43(a) read with section 66 of Information Technology (Amendment) Act, 2008 and under Section 379 & 406 of Indian Penal Code, 1860, a hacker can be punished. Before the 2008 Amendment Act, Hacking was punishable under Section 66 of the IT Act with upto three years of imprisonment or fine which may extend upto two lakh rupees, or both. If such crime is proved then for such hacking offence, the accused is punished under IT Act, for imprisonment, which may extend to three years or with fine, which may be extended to five lakh rupees or both. Hacking offence is considered as a cognizable offence, it is also a bailable offence.

Credit Card Fraud

Online credit card frauds take place when customers use their credit card or debit card for any online payment and another person, with mala-fide intentions, use such card details and password by hacking and misusing it for online purchases using the customers hacked card details or action of a fraud made by an devil34. The hacker can misuse the credit card by impersonating the credit card owner when electronic transactions are not secured.

Keystroke Logging or Keylogging

Key logging is a method by which fraudsters record actual keystrokes and mouse clicks. Key loggers are “Trojan” software programs that target computer‟s operating system and are “installed” via a virus. These can be particularly dangerous because the fraudster captures user ID and password, account number, and anything else that has been typed.

Viruses

A virus is a program that infects an executable file and after infecting it causes the file to function in an unusual way. It propagates itself by attaching itself to executable files like application programs and operating system. Running the executable file may make new copies of the virus. On the other hand, there are programs that can copy themselves, called worms which do not alter or delete any file, but only multiply itself and send the copy to other computers from the victim‟s computer.

Spyware

Spyware is the number one way that online banking credentials are stolen and used for fraudulent activities. Spyware works by capturing information either on the computer, or while it is transmitted between the computer and websites. Often times, it is installed through fake “pop up” ads asking to download software. Industry standard Antivirus products detect and remove software of this type, usually by blocking the download and installation before it can infect the computer.

Watering hole

“Watering hole” cyber fraud is considered to be a branch arising from phishing attacks. In watering hole, a malicious code is injected onto public web pages of a website which is visited only by a small group of people. In a watering hole attack situation, when the victim visit the site

injected with malicious code by attackers, the information of such victim is then traced by the attacker. In phishing attack, victim himself gives away information innocently whereas in watering hole the attacker waits for the victim to visit the site. There can be an increase in watering hole incidents when there is more misuse and exploitation of zero-day vulnerabilities in various software programs like Adobe Flash Player or Google Chrome. Cyber criminals in watering hole use the kits available in black market to infect, inject and configure a website which may be new or updated to lure people to provide them details. The site which is to be used for an attack is usually hacked by the attackers‟ months before the actual attack. They use professional methods to perform such act. Therefore it becomes difficult for cyber-crime cells to locate such infected website. Watering hole is thus a method of surgical attack where the hackers aim to hit only certain specific group of people in the internet and in comparison to phishing, it is less ear splitting.

Credit Card Redirection and Pharming

Pharming is linked with the words, „farming‟ & „phishing‟. In Pharming a bank‟s URL is hijacked by the attackers in such a manner that when a customer log in to the bank website they are redirected to another website which is fake but looks like an original website of the bank. Pharming is done over Internet and Skimming is another method which occurs in ATMs.

DNS Cache Poisoning

DNS servers are deployed in an organization‟s network to improve resolution response performance by caching previously obtained query results. Poisoning attacks against a DNS server are made by exploiting vulnerability in DNS software. That causes the server to incorrectly validate DNS responses that ensure that they‟re from an authoritative source. The server will end up caching incorrect entries locally, and serve them to other users that make the same request. Victims of a banking website could be redirected to a server managed by criminals who could use it to serve malware, or to induce bank customers to provide their credentials to a copy of a legitimate website. If an attacker spoofs an IP address; DNS entries

for a bank website on a given DNS server, replacing them with the IP address of a server they control, makes an attacker able to hijack customers.

Malware based-attacks

Malware based-attacks are one of the most among hazardous cyber threats related to electronic banking services. In such attacks, a malicious code is designed. Now-a-days, the number of malware attacks in banking sector has been increasing. Some of the infamous banking malware are Carbep, Tinba, Spyeye, Zeus and KINS. Zeus is the oldest out of these malware. It was detected in July 2007 when the information was lost and stolen from United States Department of Transportation. There are other malwares which have been identified in previous years to commit bank fraud on a large scale.42 It has been noticed that almost every virus has two features, one, that they secure a backdoor entry into the system and they steal credential information of a user.

CHAPTER – IV

DISCUSSION & INTERPRETATION

CHAPTER – IV

DISCUSSION & INTERPRETATION

4.1. DATA ANALYSIS AND INTERPRETATION IN ABROAD

26 Bank cases studied under the head of cyber-attacks. Findings are demonstrated in Table 2.

Table 2: Demonstrating the major Cyber-attacks on financial institutions from (2010-2018).

Cyber-attacks on Financial Institutions 2010-2018 Demographics* Type of Loss					
		Type of Loss			Total
		Financial Loss	Data Stealing	Customer Frustration	
Demographics	US	4	1	6	11
	Europe	2	1	2	5
	Asia	6	3	0	9
	Africa	-			-
	Australia	0	1	0	1
Total		12	6	8	26

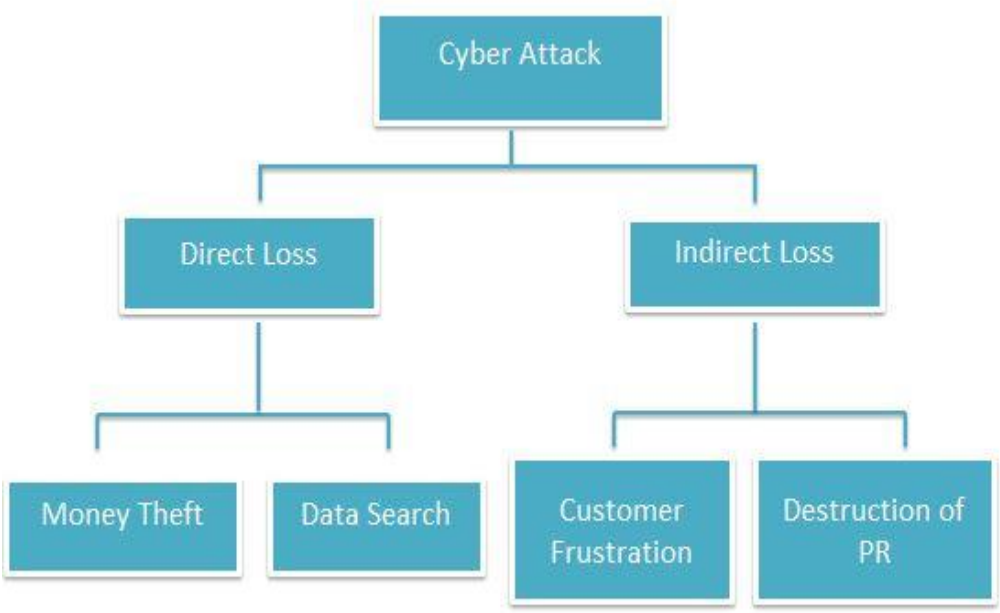
DISCUSSION

Evidences conclude that cyber-attacks impact on financial institutions in the following ways:

- Direct Loss
- Indirect Loss

Direct and indirect loss can be further classified in to two categories. Table 2 demonstrates categorized losses suffered by financial institutions as a consequence of cyber-attack (Figure 1).

Figure 1: Demonstrating the possible losses as a consequence of cyber-attack on financial institution.



- Cyber criminals gain remote access to the systems where they can administer all data.
- They can cause a financial loss (by making false transaction).
- They can steal the confidential information and they can sale it, even they can use it for spying or terrorism.
- They can target customers by attacking on organization. It may result into customer frustration or customer identity theft.
- Organization's public image can be destructed for insufficient information security compliance.

From the above findings in Table 2, it can be noted that financial losses are highest in ranking followed by customer frustration and data breach. In addition to the above it can be noted cyber-attacks on US banks in the duration 2010-018 were more frequent among all demographics. African banks are also one of the victims of cyber-attack but no individual bank case found from secondary data that could be included in this study but overall sufferings are mentioned above.

4.2. DATA ANALYSIS AND INTERPRETATION IN INDIA

Reserve Bank of India (RBI) is the regulatory body over banking in India. It keeps close eye on the banking operations

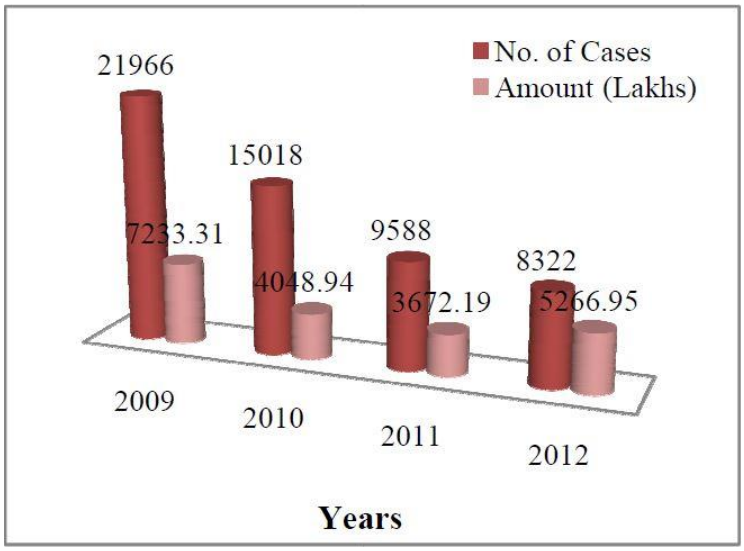
However, electronic and online data processing leaves plenty space for manipulations. The Reserve Bank of India (RBI) has recently published the detail of cyber frauds (frauds relating to ATMs/Debit Cards/ Internet Banking and Credit Cards) in Scheduled Commercial Banks. Table 4 shows the detail as under:

Table 3

Cyber Crimes in Scheduled Commercial Banks in from 2009-2012

S.No.	Calender Year	Total Cases Reported	Amount Involved (in Lakhs)
1	2009	21966	7233.31
2	2010	15018	4048.94
3	2011	9588	3672.19
4	2012	8322	5266.95

Figure-2: Graphical Presentation of Table-3



The Table and chart shows reducing number of reported cases. The amount is also reducing, but the year 2012 shows an increase. The number of cases fell by 31.6%, 36.2% and 13.2% in the year 2010, 2011 and 2012respectively. The amount involved also came down by 44.0%, 9.3% in 2010 and 2011, but in 2012 it rose by 43%.

Comparative Analysis

The data have been analysed to reveal comparative status of fraud cases in terms of numbers and amount involved. The study focuses two kinds of comparisons. i. inter sector (banks within same sector) comparison and; ii. Inter banking (between sectors) comparison.

i. Inter Banking Sector Comparative Analysis

Banks belonging to the same sector, i.e. public, private, and foreign sector have been presented in different tables along with their data in terms of number of cybercrime cases and their monetary values.

TABLE 4

Detail of Calendar Year wise Cyber Frauds in Public Sector Banks (Amount in Lakh)

		2009		2010		2011		2012	
S.No.	Bank Name	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved
1	Allahabad Bank	0	0	0	0	1	3.3	0	0
2	Aandra Bank	0	0	1	31.85	1	0.52	0	0
3	Bank of Baroda	6	6.8	5	12.4	5	31.82	3	62.45
4	Bank Of India	5	5.21	2	14.61	2	54.49	7	15.82
5	Bank Of Maharashtra	4	3.55	4	4.69	2	2.9	3	105.26
6	Bank Of Rajasthan Ltd.	0	0	1	0.31	0	0	0	0
7	Canara Bank	6	1.3	0	0	1	0.6	1	10.24
8	Central Bank of India	2	0.84	2	2.1	0	0	0	0
9	Corporation Bank	2	0.72	2	6.21	5	6.44	47	21.69
10	Dena Bank	0	0	1	2.07	1	0.53	0	0
11	Firstrand Bank	0	0	0	0	0	0	14	4.8
12	IDBI Bank Ltd.	24	16.29	13	15.29	50	44.64	87	203.04
13	Indian Bank	0	0	1	1.4	1	0.41	4	20.9
14	Indian Overseas Bank	2	3.9	3	1.44	10	176.03	0	0
15	Oriental Bank Of Commerce	0	0	1	4.75	0	0	0	0
16	Punjab National Bank	33	50.15	108	248.64	28	170.19	14	99.43
17	SBBJ	2	6.66	2	0.15	2	3.49	1	49.32
18	State Bank Of Hyderabad	0	0	0	0	4	63.33	6	50.52
19	State Bank Of India	0	0	0	0	2	14.62	0	0
20	State Bank Of Indore	1	0.8	0	0	0	0	0	0
21	State Bank Of Mysore	0	0	1	1.01	0	0	0	0
22	State Bank Of Patiala	0	0	0	0	4	80.45	2	31.42
23	State Bank Of Travancore	0	0	0	0	6	10.3	3	3.2
24	Syndicate Bank	2	0.53	1	2.32	1	0.56	2	7.87
25	UCO Bank	2	50.8	1	1.6	0	0	4	31.22
26	Union Bank Of India	5	10.45	7	19.22	2	7.86	9	70.17
27	United Bank Of India	1	1.37	0	0	0	0	6	32.86
28	Vijay Bank	0	0	0	0	0	0	1	8.4
Grand Total		97	105.81	156	370.12	128	672.68	214	828.63

Interpretation: It can be observed from table- 5 that the numbers of fraud cases in public sector banks were small but they rose during the four years period with a small drop in 2011. The amount involved had no relationship with this fall and had a rising tendency. In year 2009, PNB recorded the highest number and amount of cybercrime cases followed by IDBI bank. In 2010, PNB showed highest number of cases followed by IDBI, but amount wise. PNB was followed by Andhra Bank, Union Bank of India and IDBI respectively. IDBI crossed PNB in 2011 in terms of cases, but amount wise. Indian Overseas, PNB and Bank of Patiala witnessed a substantial rise. In 2012, IDBI came on top followed by Corporation Bank

and PNB. In terms of money involved, IDBI, Bank of Maharashtra and PNB recorded highest positions respectively. Figure-3 also describes the story.

Figure 3

Graphical Presentation of Table-4

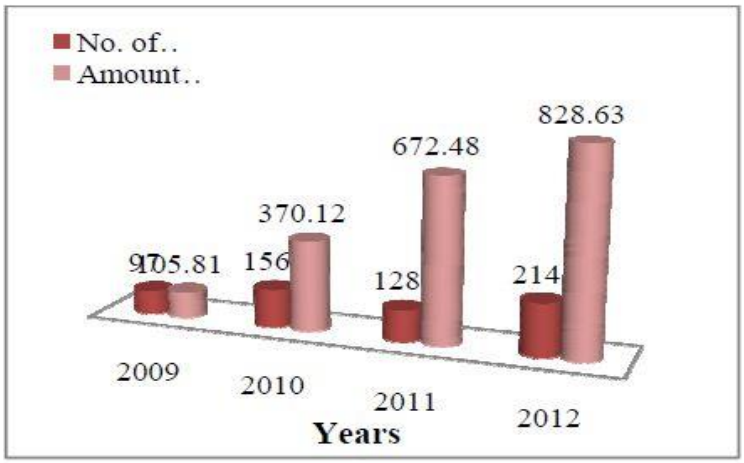


TABLE 5

Detail of Calendar Year wise Cyber Frauds in Private Sector Banks (Amt.t in Lakh)

		2009		2010		2011		2012	
S.No.	Bank Name	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved
1	Axis Bank Ltd.	20	110.58	14	44.59	23	209.59	85	1225.41
2	Development Credit Bank	2	0.96	2	0.3	0	0	0	0
3	Dhanlaxmi Bank Limited	0	0	3	2.29	1	3.02	4	1.09
4	Fedral Bank Ltd.	0	0	2	20.5	0	0	3	83.69
5	HDFC Bank Ltd.	211	165.58	208	125.98	386	276.68	525	409.56
6	ICICI Bank Ltd.	15666	3731.95	9811	1920.28	6013	1096.67	3428	676.51
7	Industrial Bank Ltd.	0	0	3	7.59	3	1.19	2	4.61
8	Jammu&Kashmir Bank	1	4.51	2	6.58	0	0	1	13.88
9	Karur Vysya Bank Ltd.	0	0	1	23.14	0	0	0	0
10	Kotak Mahindra Bank Ltd.	57	75.26	31	29.63	52	33.11	78	67.64
11	Lakshmi Vilas Bank Ltd.	0	0	0	0	0	0	1	10
12	South India Bank Ltd.	1	2.47	1	0.54	2	0.84	2	0.49
13	Tamilnad Mercantile Bank	0	0	0	0	1	0.27	1	1.49
14	The Royal Bank Of Scott.	142	141.3	51	44.52	46	49.35	14	12.1
Grand Total		16100	4232.61	10129	2225.94	6527	1670.72	4144	2506.47

Interpretation: Data of table-6 reveals that private sector banks had the largest share in banking cyber frauds not only in number of cases but also in terms of money. But the noticeable point is their falling trend. The number of cases came down from 16100 in 2009 to 4144 in 2012. Similarly the amount also came down from 4232.61 lakhs in 2009 to 1670.72 in 2011, but it again rose to 2506.47 in 2012. However, overall a declining trend has been observed in cyber frauds in private sector bank.

ICICI bank had a highest position in cyber frauds during this four years period showing a very high number of cases and large money involved. HDFC and Axis Banks followed the position respectively with a sudden rise in value by Axis Bank in 2012. This can be easily understood by Figure-4.

Figure 4

Graphical representation of Table-5

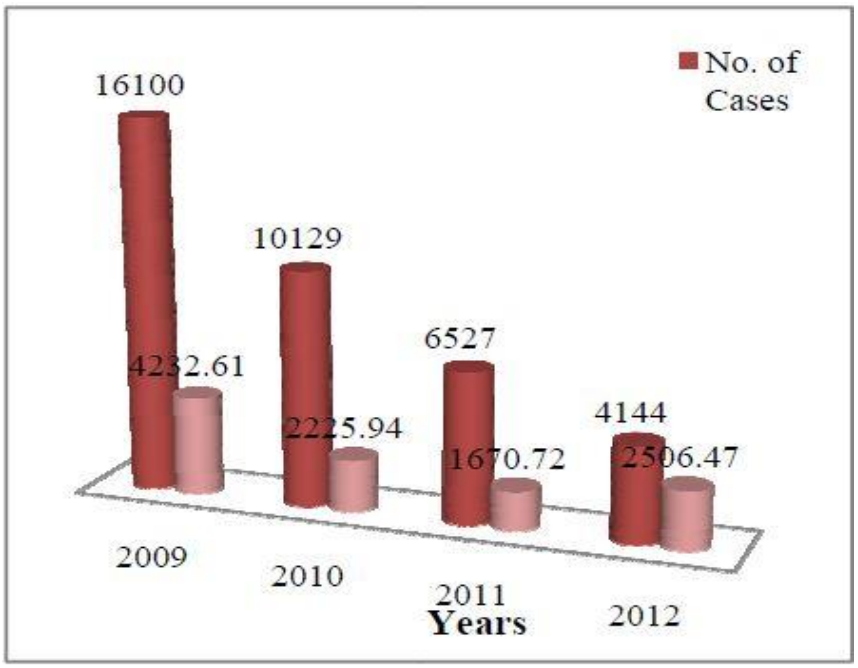


TABLE 6

Cyber Frauds in Foreign Banks (Calendar year wise year detail)

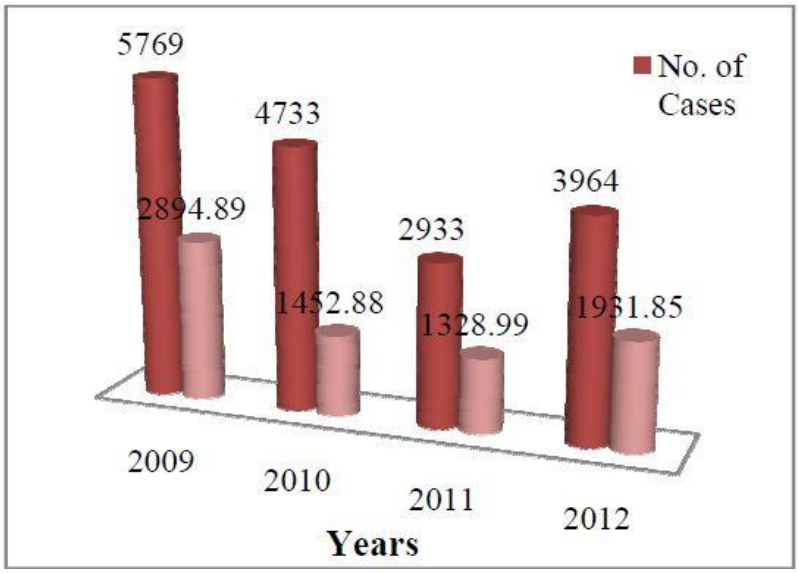
		2009		2010		2011		2012	
S.No.	Bank Name	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved
1	American Express Banking Corp.	980	904.57	819	360.75	908	522.76	1231	816.99
2	Barclays Bank Plc	35	21.68	48	8.38	14	6.03	7	1.11
3	Citi Bank N.A.	1226	773.18	925	521.27	774	420.01	1504	690.32
4	Deutsche Bank (Asia)	61	116.64	35	81.94	9	13.67	2	34.74
5	Hongkong& Shangahai Banking Corporation Ltd.	3093	722.45	2520	293.02	793	181.41	709	180.73
6	Standard Chartered Bank	374	356.37	386	187.52	435	185.11	511	207.96
Grand Tortal		5769	2894.89	4733	1452.88	2933	1328.99	3964	1931.85

Interpretation: The status of cybercrime cases in foreign bank can be observed from table-7, which shows that cyber frauds are there in such banks to a great extent. Even after somewhat declining trend, the year 2012, like in case of public and private sector banks, has shown a rise in number and amount of fraud cases.

The table also shows that HSBC, which had the largest share in 2009, has corrected the situation up to 2012 while two other leading banks Citibank and American Express have surpassed HSBC. Figure-5 portrays the same.

Figure 5

Graphical representation of Table-6

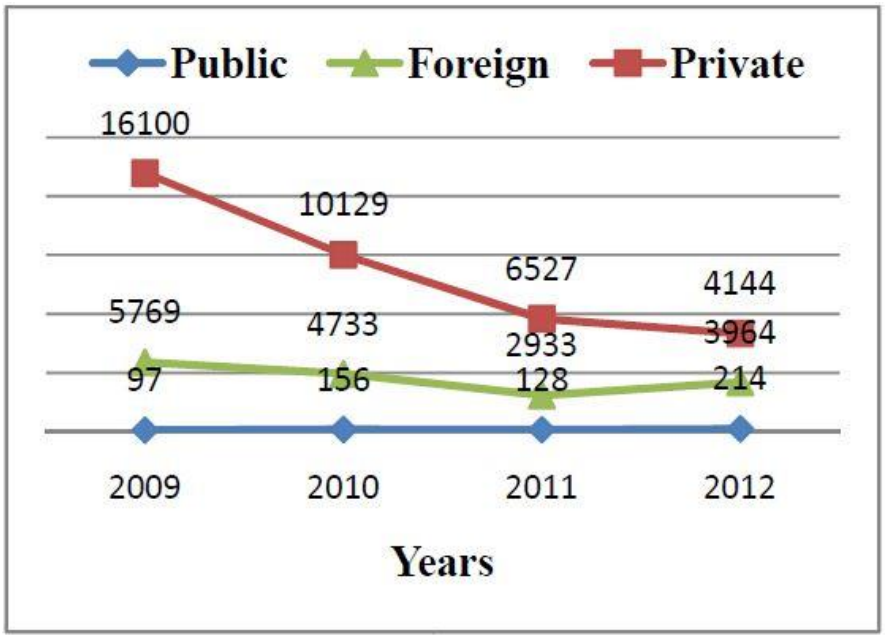


ii. Inter Banking Sector Comparative Analysis

Banking cyber fraud data of public, private and foreign sector banks have been depicted in Figure-6 and Figure-7

Figure 6

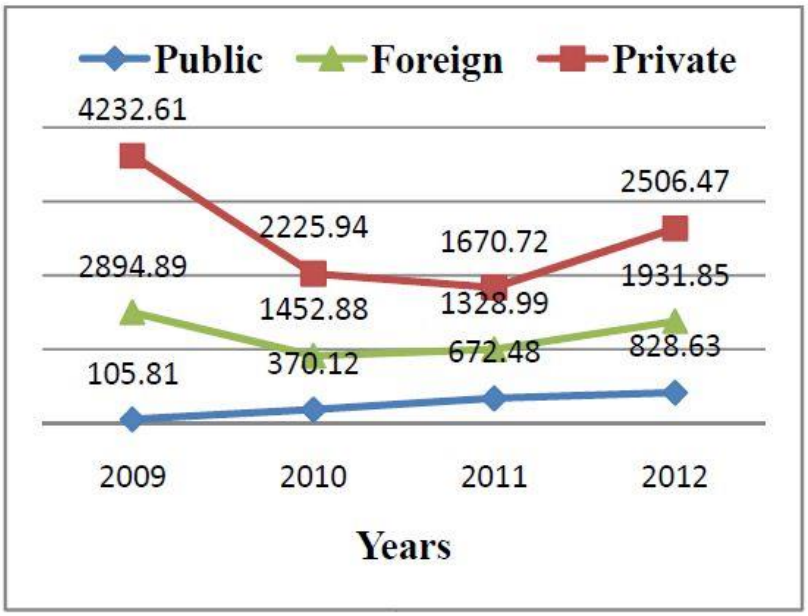
Banking Sector wise No. of Cases



Interpretation: If look at Figure-6, which portrays the number of fraud cases from 2009 to 2012, it is obvious that private sector banks have gone far away recording very large number of cases. Foreign banks are no different either. Monetary loss wise also both kinds of banks have made a bad picture. However, public sector banks demonstrate very nominal number of cases. But, a substantial drop has been noticed in the cases in both, private and foreign banks, which suggests major and stricter check over the operations.

Figure 7

Banking Sector wise Amount Involved (in Lakhs)



Monetary involvement in fraud cases has been shown in Figure-7. Here also both private sector banks and foreign banks are much ahead of public sector banks. After a declining trend up to 2011, the value again ascended in 2012.

4.3. TECHNIQUES USED IN CYBER CRIME IN BANKING SECTOR

There are few techniques in which a cybercrime can be committed. Here we have to aware how these crimes will be affected our computer privacy. In this section, we talk about a few common tools and techniques used by the cyber criminals. This isn't a comprehensive list by any ways, but will give you a complete picture of the gaps in networks and security systems, which can be misused by attackers, and also their possible causes for doing such crimes.

1. **Hacking**: In simple, hacking is an action committed by an intruder by accessing our computer system without our permission. Hackers are primarily computer programmers, who have a superior understanding of systems and commonly misuse

this knowledge for tricky reasons. They're usually technology experts who have expert-level skill set in one particular software program or language.

2. **Virus:** Viruses are computer programs which will spread like a biological virus or infect a computer or files, and have a tendency to combine other systems on a network. They interrupt the computer operation and affect the database either by altering it or by removing it altogether. They just reproduce until they consume up all available memory in the computer.

3. **Logic bombs:** Logic bomb, also called as "slag code", is a horrible piece of code which is intentionally inserted into software to execute a malicious task when generated by a specific event.

4. **Denial-of-Service attack:** Attack is obvious attempt by attackers to deny service to prospective users of that service.

5. **Phishing:** This technique is used for removing confidential information such as credit card numbers and username passwords. Phishing is typically carried out by email tricking. The malware would have installed itself on the computer and stolen private data.

6. **Data diddling**: Data Diddling is an unlawful altering of data before or during entry into a computer system, and then altering it back after processing is completed. Using this technique, the attacker may change the expected outcome and is difficult to track.

7. **Keystroke Logging or Key logging**: Key logging is a process by which attackers' record actual keystrokes and mouse clicks. Key loggers are "Trojan" software programs that aim at computer's operating system and are "installed" via a virus. These are very dangerous because the fraudster captures user ID and password, account number, and anything else that has been typed by the user.

8. **Spyware:** Spyware is a technique to stolen online banking credentials of the users for fraudulent activities. Spyware works by capturing information either on the computer while it is transforming between the computers and websites.

9. **Watering hole:** "Watering hole" cyber fraud is considered to be a branch arising from phishing attacks. In watering hole a malicious code is injected onto public web

pages of a website which is visited only by a small group of people. In a watering hole attack situation, when the victim visit the site injected with malicious code by attackers the information of such victim is then traced by the attacker

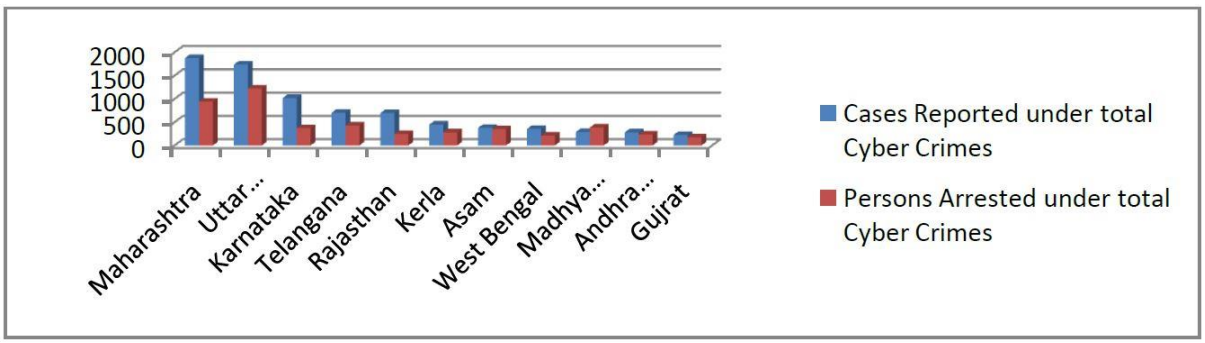
10. **Credit Card Redirection and Pharming:** Pharming is connected with the words, 'farming' & 'phishing'. In Pharming a bank's URL is hijacked by the attacker in such a manner that when a customer log in to the bank website they are redirected to another website which is false but looks like an original website of the bank. Pharming is done over Internet and Skimming is another method which occurs usually in ATMs.

11. **DNS Cache Poisoning**: DNS servers are deployed in an organization's network to improve decision response by caching before obtained query results. Poisoning attacks against a DNS server are made by exploiting exposure in DNS software. That causes the server to wrongly validate DNS responses that ensure that they're from an authoritative source. The server will end up caching incorrect entries locally, and serve them to other users that make the same request.

4.4. Current Status of Cyber-crimes in Banking Sector

Incident of Cognizable Crime under IT Act During 2014

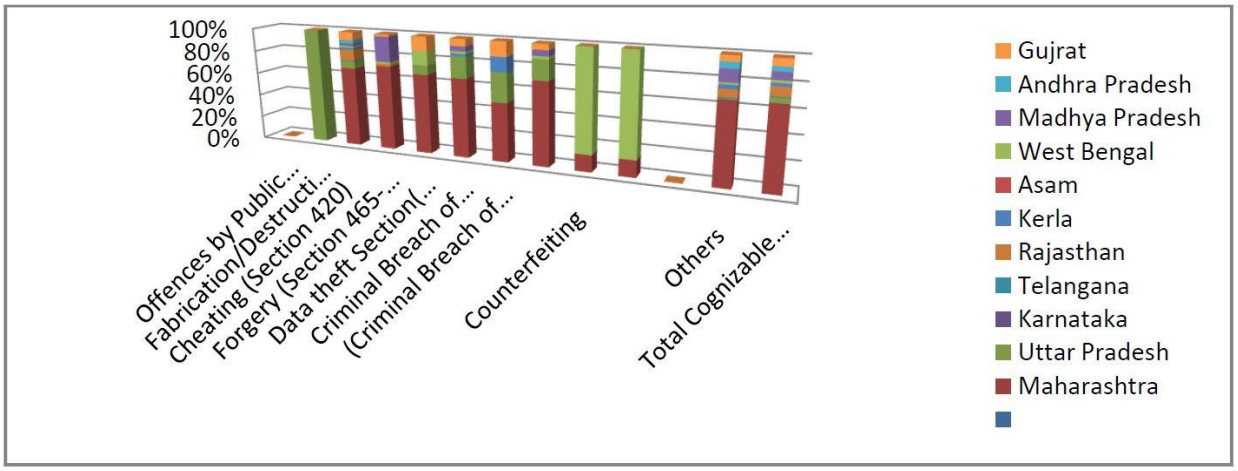
1. **Cases Reported and Persons Arrested under Cyber Crime in 2014**



(Source: Crimes in India 2014 Statistics)

The above graph shows the information about cybercrime cases registered and persons arrested during 2014.From the above graph it is seen that maximum cybercrimes cases are registered in Maharashtra state (1879). But compare to registration of cybercrimes cases less persons are arrested (942). Uttar Pradesh is at the second position for committing the cyber-crimes (1737) and maximum persons are arrested (1223).Gujarat state is at the bottom for committing the cyber-crimes.

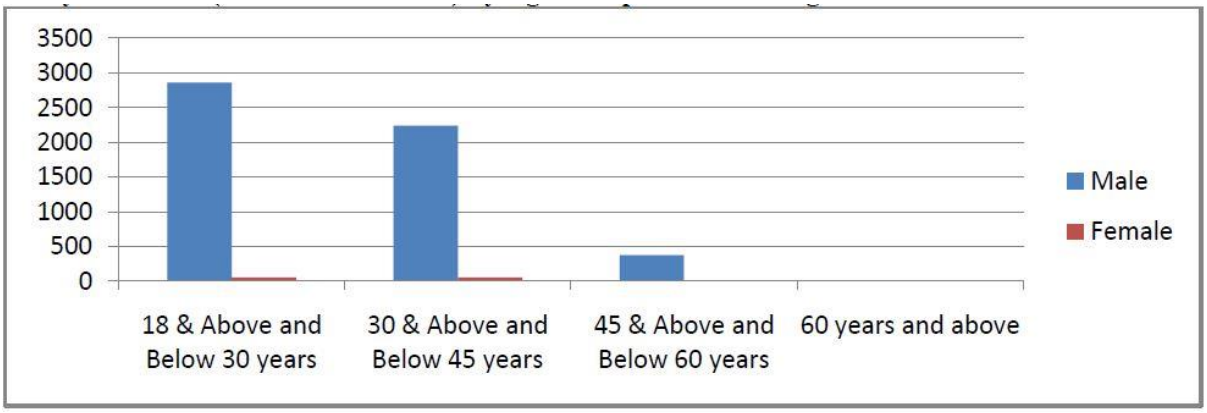
2. **Incidence of Cognizable Crimes under IPC (involving Computer As Medium/Target) During 2014**



(Source: Crimes in India 2014 Statistics)

Maharashtra state is at the top for committing cognizable crimes under IPC (involving Computer As Medium/Target) during 2014. Under this cheating under section 420 (671), Forgery under Section 465- 469,471& 477A (37), Data theft under section 379 to 381 (17), Criminal Breach of Trust/Fraud– debit cards & others under section 406, 408, 409 (33) are involved. Rajasthan is at second position (145). At the bottom position Karnataka state is with only 2 cognizable crimes.

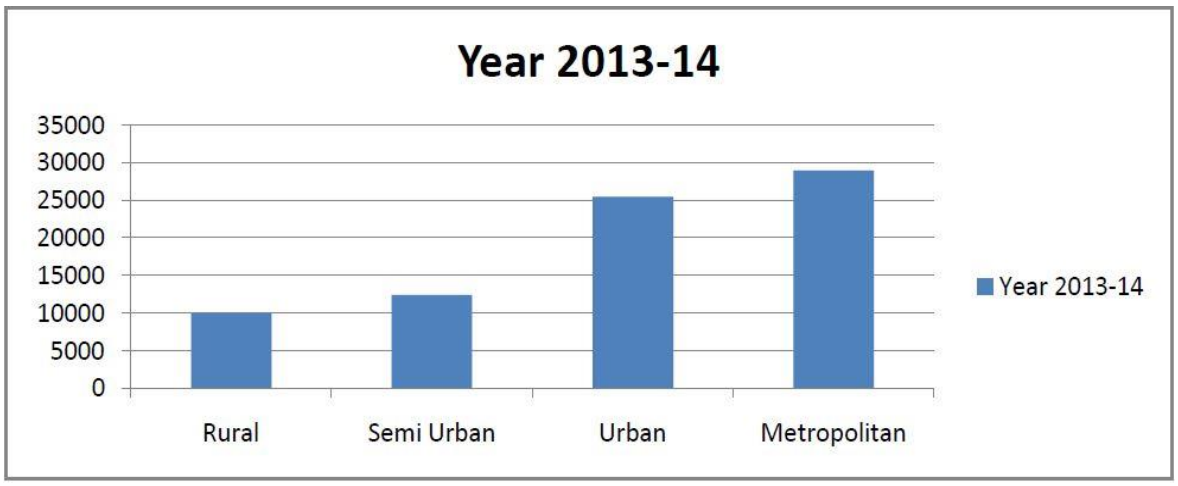
3. Total Cyber Crimes(IT Act + IPC +SLL) by Age Groups & Sex During 2014



(Source: Crimes in India 2014 Statistics)

The above graph shows the total cybercrimes under IT Act, IPC, SLL by Age Groups & Sex During 2014. It is seen that the maximum involvement of committing the cybercrimes under 18 & Above and Below 30 years age group of male (2859) is found. And only 54 females under same age groups are found. Comparative to other age groups (30 & Above, 45 & Above and 60 years and above) maximum involvement for committing the cybercrimes is found under 18 & above and below 30 age group. The involvement of the persons in 60 years & above age group is also found. As compared to the male in all age groups the female involvement for committing cybercrimes is very less.

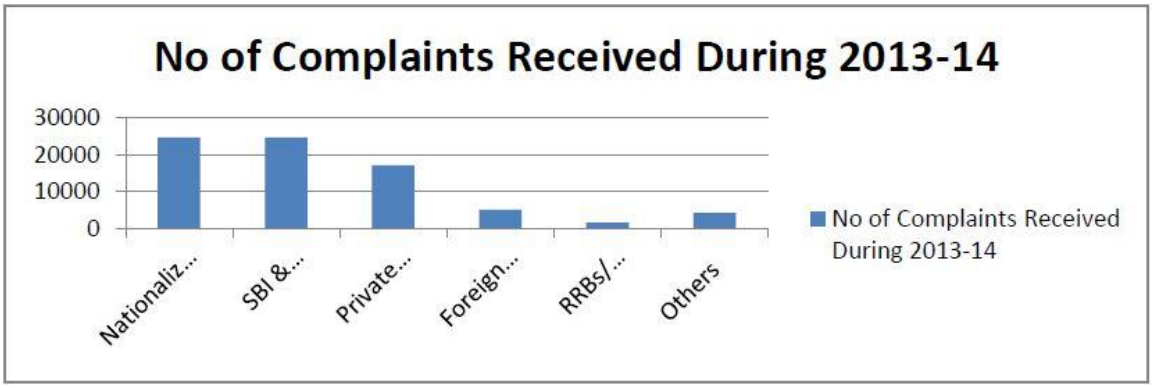
4. Population group-wise distribution of complaints received to RBI



(Source: Annual Crime Report of RBI 2013-14)

According to RBI report the distribution of complaints received from metropolitan area (28884) is more than compare to urban, semi urban and rural. Very less complaint are received to RBI from rural area (9927).

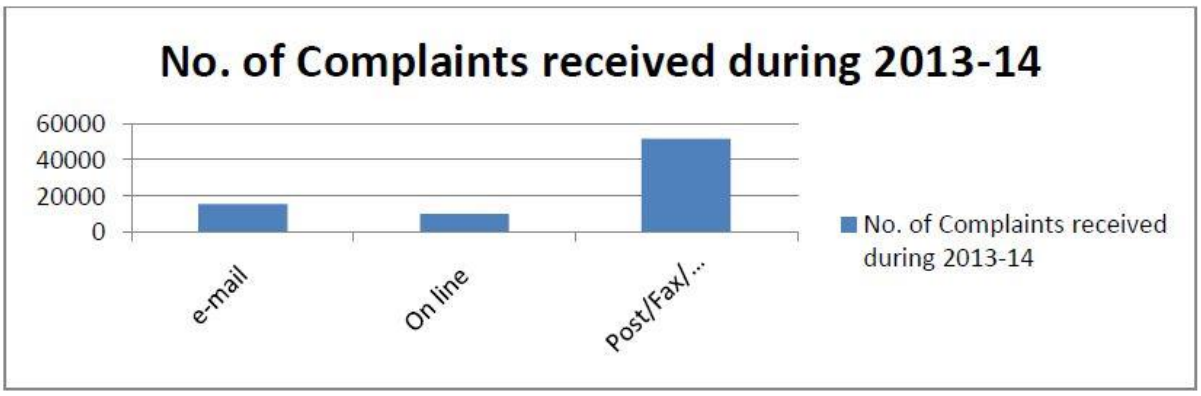
5. **Bank group-wise classification**



(Source: Annual Crime Report of RBI 2013-14)

The above graph shows the bank group wise classification of complaints received during 2013-14. It is seen that more complaints are received from Nationalized Banks group (24391) which follows SBI & Associates(24367), Private Sector Banks(17030), Foreign Banks(5016) and Others(4179). Very less complaint are received from RRBs/ Scheduled Primary Urban Co-op. Banks (1590).

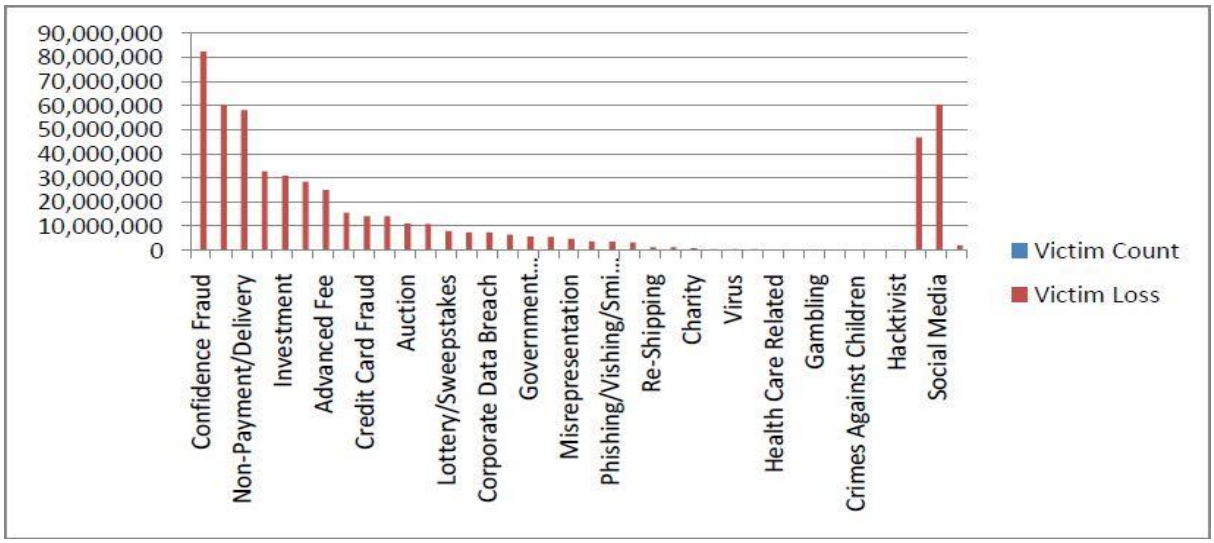
6. **Receipt of complaints Mode-wise**



(Source: Annual Crime Report of RBI 2013-14)

In 2013-14 Maximum complaints are received to the RBI by Post/Fax/Courier and hand delivery (51607). Very less people are using online and e-mail facility to report the complaints to the RBI.

7. Six Month Statistics by Crime Type June 1, 2014 – December 31, 2014



(Source: Annual Crime Report of RBI 2013-14)

In 2013-14 Maximum complaints are received to the RBI by Post/Fax/Courier and hand delivery (51607). Very less people are using online and e-mail facility to report the complaints to the RBI. Fraud (Victims-7783 and Loss-$14236939), phishing(Victims-6495 and Loss-$3560332), virus(Victims-421 and Loss-$398979),Malware(Victims-819 and Loss-$314764),Denial of services(Victims-417 and Loss-$273761), Gambling(Victims-48 and Loss-$134962), Hacktivist (Victims-40 and Loss-$1058),Personal data breach(Victims-5145 and Loss-$5493229), corporate data breach(Victims-393 and Loss-$7316372), virtual currency(Victims-392 and Loss-$1972312).

8. Cases Registered Under Cyber Crimes Categorized By Motives and Suspects from 2010 – 2015

Motives and Suspects	2010	2011	2012	2013	2014	2015
Revenge/settling	38	70	87	112	285	304
Greed/Money	161	306	624	821	1736	3855
Extortion	24	27	48	73	199	295
Cause Disrepute	36	82	117	148	272	387
Prank/ satisfying of gaining control	13	77	45	39	110	214
Fraud/Illegal gain	266	487	668	1116	495	1119
Total	**538**	**1049**	**1589**	**2309**	**3097**	**6174**

(Source: National Crime Report 2016)

9. Incidence of Cyber Crimes cases Registered during 2010-2015

Crime Type	2010	2011	2012	2013	2014	2015
Tampering Computer Source Document	64	94	161	137	89	88
Loss/ Damage to computer resource/utility	346	826	1440	1966	4192	4154
Hacking	164	157	435	550	784	1081
Obscene publication/ Transmission in electronic form	328	496	589	1203	758	792

(Source: National Crime Report 2016)

10. Cases Registered Under Cyber Crimes Cauterized by Motives and Suspects from 2010-2015

Motives and Suspects	2010	2011	2012	2013	2014	2015
Revenge/settling	38	70	87	112	285	304
Greed/Money	161	306	624	821	1736	3855
Extortion	24	27	48	73	199	295
Cause / Disrepute	36	82	117	148	272	387
Prank / satisfying of gaining control	13	77	45	39	110	214
Fraud / Illegal gain	266	487	668	1116	495	1119
Total	**538**	**1049**	**1589**	**2309**	**3097**	**6174**

(Source: National Crime Report 2016)

From the above tables we can understand that the financial services sector faces specific challenges of its own. Banks are struggling with the decentralization of their services through digitization. The growth of Fintech throws pressure on the banking sector where the technology and e-commerce companies are now competitors to and partners with banks. Banks have to believe that having an effective digital strategy is one of the important priorities. Accompanying this will be the change management of the shift. Technology on its own improves nothing. But people using technology competently and effectively can make a big difference.

CHAPTER – V

CONCLUSION, AND SUGGESTIONS

CHAPTER - V

CONCLUSION AND SUGGESTIONS

5.1. Conclusion

The present study was design to study the:

1. To study the working operation of cybercrime.
2. To study technique used in cybercrime in banking sector.
3. To Study meaningful analysis of the data belonging to banking cybercrime of different banking sectors.
4. To study the current status of cybercrimes in banking sector.
5. To identify the preventive measures to control frauds.

After studying the available data, a careful analysis and interpretation of data has been carried out in the previous chapters on the basis of data analysis and interpretation finding, conclusion and suggestions for further research for the context of the study are presented in this chapter.

This Study showed a bigger share of private and foreign bank crime related to online banking, ATM cards and other digital banking transactions. Banking cybercrime in the country are the result of introductory phase of banking technology like ATM, Online Banking, and EFT etc. Which need time for people market and technology to get matured.

In the analysis researcher found that cybercrime is a big concern all over the world. All types of crime like Phishing and Vishing, Hacking is prevalent in all countries. Majority of cybercrimes in bank have resulted out of hacking and identity theft.

Banks can prevent these crimes to some extent because they cannot stop users to use their online banking and cannot check their computers whether they are free from malware or not. The security of the customer is at a huge risk because it has become very easy to hack their personal

detail. Bank fraud also shows that the customers engage in internet banking is not alert and not have sufficient knowledge of cybercrimes.

It is also shows indicated in the analysis crime rates in the metropolitan areas is more than compare to urban, semi-urban, and rural areas. Analysis also indicates that numbers of fraud cases in public sector banks were small in comparison to private sector bank. ICICI bank has a highest position in cyber frauds, HDFC and Axis Bank followed the position next to ICICI.

It is banks responsibility to aware and educates customers time to time about the prevailing threats in the market. Negligence by customer and IT sector is the another reason for cybercrime.

In India the cybercrimes are increasing considerably. The crimes such as social media, credit card fraud, phishing, and virus, Malware, Denial of services, Gambling, Personal data break, corporate data break and virtual currency are frequently done by cyber criminals. Most of the cybercrimes are devoted at nationalized banks. Maximum sufferers are suffered from money loss and data loss. The internet is the medium for transforming of huge information, it is essential to take certain precautions while sharing information through systems. It is very vital to educate users of internet regarding these cybercrimes and explain them what precautions they have to take to safeguard their computers as well as personal data. In this regard banks may have to take utmost care regarding their firewall and anti – virus systems.

While each bank thinks distinctively on adopting various considerations it is imperative to assume that the theme remains the same for various banking channels:

Internet Banking: Security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.

Mobile Banking: It should be ensured that mobile applications are up to date and should be tested. Latest hardening standards could be implemented.

Wallet Transactions: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.

ATM Security: Biometrics like eye-retina, voice scan or fingerprint scan should be introduced by Banks.

Some of the Cyber Security Attacks on Banks

Banks are exposed to a number of cyber security attacks. RBI in identifies Phishing, Cross site scripting, Vishing, Cyber-Squatting, Bot networks, E-mail related crimes, Malware, SMS spoofing, Denial of service attacks, Pharming, Insider threats as the emerging information security attacks on banks.

Phishing

One of the most common cyber frauds is ―Phishing‖. Phishing is an attack in which an attempt is made to obtain sensitive information of user such as usernames, passwords, credit card details, etc. by an attacker by pretending to be a reliable body in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging in which users are asked to click on a link usually for securing their accounts. The users are then directed to fraudulent websites which look alike the original banking website so that the user is deceived and is asked to enter his personal information such as usernames, passwords, credit card details, etc. Once the user enters his/her personal information, the fraudster then has access to the customer's online bank account and to the funds contained in that account. There are a variety of tools and techniques used by phishers which serve a variety of functions, including email delivery, phishing site hosting, and specialized malware. These tools include Botnets, Phishing Kits, Abuse of Domain Name Service (DNS), Technical Deceit, Session Hijacking and Specialized Malware.

A phishing incident was reported in Hyderabad, which was in the name of India’s central bank RBI in which the phishing email said that RBI had launched a new security system and asked users to click a link which redirected users to a fake website. It asked users to enter their online bank credentials including card numbers and the secret three digit CVV number, among others. RBI has cautioned people that it has not launched any such software as soon as it came to know about it.

Cross site scripting

Cross-site scripting (XSS) is a kind of cyber security vulnerability usually found in web applications and they allow code injections by malicious web users into the web pages that are viewed by other users. Examples of such code include client-side scripts, HTML code, etc. A cross-site scripting vulnerability can be exploited by attackers to bypass access controls. Their

impact ranges from a petty nuisance to a significant security risk, depending on the sensitivity of the data that is handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

Vishing

Vishing is a cyber-attack in which social engineering and Voice over IP (VoIP) are used to access the private and financial information from the public for getting financial reward . It combines "voice" and ―phishing‖. Vishing is an illegal practice where an attacker calls a user and pretends to be from a bank in which the user has an account. He usually asks to verify the user's account information (stating that user's account has been suspended, etc.) and once the user gives his credentials such as username, password, credit card number, etc., the attacker has easy access to the user's account and the money in it. There has also been a theft of payment card data of the customers of U.S. banks by various vishing attacks. In an attack in 2014, customers of a midsize bank received SMS text messages which claimed their debit card was deactivated and asked users to provide the card and PIN numbers to reactivate it.

Cyber squatting

Cyber-squatting is a process in which a famous domain name is registered and then it is sold for a fortune. Cyber Squatters register domain names which are similar to popular service providers' domains so as to attract their users and benefit from it. Some countries have specific laws against cyber-squatting that are beyond the normal rules of trademark law. For example, the United States has the U.S. Anti-cybersquatting Consumer Protection Act (ACPA) of 1999 which provides protection against cybersquatting for individuals and also owners of distinctive trademarked names. The Washington Post reported in 2007 that Dell filed a lawsuit against Belgium Domains, Capitol Domains, and Domain Doorman for cyber-squatting and typo-squatting and dellfinacncialservices.com was one of the domains that was cited.

Bot Networks

Bots are programs that infect a system to provide remote command and control access via a variety of protocols, such as HTTP, instant messaging, and peer-to-peer protocols. Several of bots under common control are commonly referred to as a ―Botnet. Computers get associated with botnets when unaware users download malware such as a ―Trojan Horse

which is sent as an e-mail attachment. The systems that are infected are termed as ―zombies. Illicit activities can be carried out with bots by the controller that include relays for sending spam and phishing emails, updates for existing malware, DDOS, etc. Bot Networks create unique problems for organizations because they can be upgraded very quickly remotely with new exploits, and this could help attackers prevent security efforts.

Malware

Malware is a maliciously crafted software program that accesses and alters the computer system without the consent of the user or owner. Malware includes viruses, Trojan horses, worms, etc. Malware can heavily influence the confidentiality, integrity and availability of the banking system. Malwares have the capability to compromise the information in the banking systems and may lead to a loss of worth millions to the bank. Malwares can target both the user's system and the bank itself. E.g.; Zeus.

Denial of Service (DOS) Attack

A DOS is an attack in which a user or an organisation is prevented from accessing a resource online. While as in Distributed denial-of-service Attack (DDOS), a specific system is targeted by a large group of compromised systems (usually called a Botnet) and makes the services of the targeted system unavailable to its users. Actually the targeted system is flooded with incoming messages which causes it to shut down and thus the system is unavailable to its users.

Although DOS attacks don't usually result in loss of information or security to a bank, it can cost the bank a great deal of time, money and customers and can also destroy programming and files in affected computer systems.

SMS Tricking

It is a relatively new technology in which a user receives a SMS message on phone which appears to be coming from a legitimate bank. In this SMS the originating mobile number (Sender ID) is replaced by alphanumeric text. Here a user may be fooled to give his/her online credentials and his/her money may be at risk of theft.

TCP/IP Spoofing

It is one of the most common forms of online camouflage. In IP spoofing, illegal access is attempted on a system by sending an email message to a victim that appears to come from a trusted machine by ―spoofing‖ the machines' IP address. IP address spoofing is a powerful technique as it can enable an attacker to send packets to a network without being blocked by a firewall. This is because usually firewalls filter packets based on sender's IP address and they would normally filter out any external IP address. However using IP spoofing, the attacker's data packet appears to come from legitimate IP address (internal network) and thus firewall is unable to intercept it. The main goal here is to obtain root access to the victim's server (here the banking system), allowing a backdoor entry path into the targeted systems.

Pharming

It is also called farming or DNS poisoning. In this attack whenever a user tries to access a website, he/ she will be redirected to a fake site. Pharming can be done in two possible ways: one is by changing host's files on a victim's computer and other way is by exploiting vulnerability in DNS server software. In January 2005, the domain name for a large New York ISP, Panix, was hijacked and legitimate traffic was redirected to a fake website in Australia. No financial losses are known. In January 2008, a drive-by pharming incident was reported by Symantec that was directed against a Mexican bank and in which the DNS settings on a customer's home router were altered after receipt of an e-mail message that appeared to be from a legitimate Spanish-language greeting-card company.

Insider Threats

With the increase in the use of information technology by banks, there is a high security risk to bank's data by insiders or employees of banks who can disclose, modify or access the information illegally. Also unintentional errors by employees can have devastating results. Healthy security processes must be used by banks to lessen such threats.

OTP Attacks

OTP(one Time Password) is a two factor authentication method in which a password is created whenever the users attempts authentication and the password is disposed of after use.

A no. of attacks can be launched on accounts that are OTP protected which are known as MIT-X methods (Man-In –The-X).

These are as follows:

Man-in –the-middle attack (MITM): Here the transmission paths of data are accessed and information is snatched in the middle of transactions.

Man-in-the-Browser attack (MITB): Here malicious code exists in the web browser and it induces users to enter credentials and other important information into a fake form.

Man-in-the-PC attack (MITPC): MITPC exploits the weaknesses in the hardware environment or operating system to steal OTP.

Security Challenges

The rapid growth of digital payments platform in India and the impetus towards a cashless economy has renewed focus on the need to strengthen cyber security posture. The following are the some of the Challenges.

Strict compliance regulations: Managing regulatory compliances has become enormously challenging for the banks. Over the past few years the volume of regulations has increased dramatically. Along with the larger banks, smaller ones too are required to fulfil the regulatory obligations

The struggle to secure customer data: There are number of ways in which violation of privacy can take place in banking sector like stolen or loss card data, unauthorized sharing of data with third parties and loss of client's personal data due to improper security measures

Third party risk: Banks need to conduct due diligence on third parties they are associated with. As per Payments card industry data security standard, third parties need to report any critical issues associated the card data environment to the bank.

Evolving cyber threat landscape: The development in technologies is leading to the latest cyber threats like next generation ransomwares, web attacks etc.

Transaction frauds: Fraud detection technologies should be in place with proper consideration of risks based on the business factors.

Secure SDLC: Banks need to incorporate SDLC security for banking products and applications.

Safety Tips for Online Secure Transaction:

1. **If the network is not properly secured**- avoid online banking, shopping, entering credit card details, etc. Check your online account frequently and make sure all listed transactions are valid
2. **Never ever click on a link-** Be extremely wary of e-mails asking for confidential information they could be phishing e-mails from fraudsters. Donot click on link given in a spam e-mail.
3. **Always delete spam-**delete spam e-mails immediately and empty the trash box to prevent clicking on the same link accidentally
4. **Beware of lotteries**- please beware of lotteries that charge a fee prior to delivery of your prize. Do not respond to lottery messages or call on the numbers provided in the text messages.
5. **Check if the website is secure**- While using a credit card for making payments online, check it if website is secure as the CVV will also be required for online transactions, is printed on the reverse of credit card. Do not provide photocopies of both sides of the credit card to anyone. It can be misused by the fraudsters for online purchases.
6. **Notify your bank/credit card issuer** - if you do not receive the monthly credit card statement on time, if a credit card is misplaced or lost, immediately inform to your bank/ credit card issuer.

Do not share bank credentials **in public** or over phone

5.2. SUGGESTIONS

1. Cyber Fraud Council in Banks

Whenever a cyber-fraud is committed the victim should report to the Cyber Fraud Council that must be set up by in each and every bank to review, monitor investigate and report about cyber-crime. In case, such Council does not take perform or refuses to perform its duty then a provision to file an FIR must be made. The matter to be brought before such council can be of any value. However, when the value is high then the Council shall act expeditiously. RBI in its 2011 Report stated that when bank frauds are of less than one Crore then it may not be necessary to call for the attention of the Special Committee Board

2. Education to Customer

The customer should be educated and made aware about various bank frauds and measures should be informed to them for safety mechanisms so that they do not fall prey as victims of cyber- crime. If a customer is conscious and report the matter of cyber-crime then in the initial stage also instances of cyber-crimes can be reduced. A customer should be made aware about the Dos and Don'ts' of E-banking. It can be done through publishing it on the bank's website, publishing in the newspaper, through advertisements, by sending SMS alerts, through poster education etc. In case a bank introduce any new policy or there are any changes which are required to be followed by all banks as per RBI then, bank must inform the customer through mails or by informing the customer through telephone. The awareness material should be timely updated keeping in mind the changes in the legislation and guidelines of RBI

3. Training of Bank Employees

Training and Orientation programs must be conducted for the employees by the banks. The employees must be made aware about fraud prevention measures. It can be done through newsletters or magazines throwing light on frauds related aspects of banks by senior functionaries, putting up 'Dos and Don'ts' in the workplace of the employees, safety tips being flashed on screen at the time of logging into Core Banking solution software, holding discussions on factors causing cybercrime and actions required to be undertaken in handling them. Employees who go beyond their call of duty to prevent cyber frauds if rewarded will also enhance the work dedication

4. Strong Encryption-Decryption Methods

E-banking activities must be dealt using Secure Sockets Layer (SSL). It provides encryption link of data between a web server and an internet browser. The link makes sure that the data remains confidential and secure. As per India, we follow asymmetric crypto system which requires two keys, public and private, for encryption and decryption of data. For SSL connection a SSL Certificate is required which is granted by the appropriate authority under IT Act, 2000. To ensure security transactions RBI suggested for Public Key Infrastructure in Payment Systems such as RTGS, NEFT, and Cheque Truncation System. According to RBI it would ensure a secure, safe and sound system of payment. Wireless security solutions should also be incorporated. In cases of Denial of Service Attacks, banks should install and configure network security devices.

5. Data protected technology adoption

Block chain is a technology that was initially developed for Bitcoin, the cryptocurrency. Block chain could reduce banks infrastructure costs by US$ 15-20 billion per annum by 2022. Block chain have the potential to transform how the business and the government work in vast variety of contexts.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. G.Gopalakrishna (2009) Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds, RBI, Mumbai, Maharashtra.

2. Moore . T, Clayton .R &Anderson .R. (2009) "The Economics of Online Crime" journal of Economic Prespective, Volume 23, Issue no.3 Summer 2009, pp3-20.

3. Aggarwal P, Arrora P, Neha, Poonam (2014) Review on cybercrime and security. International Journal of research in Engineering and Applied Sciences, p51.

4. Winter TC, Tom (2016) U.S. News

5. Susheel Chandra Bhatt and Durgesh pant (2011): Study of Indian Banks Websites for Cyber Crime Safety Mechanism, (IJACSA) International Journal of Advance Computer Science and Applications, Vol.2, No. 10, Jayshree Chavan (2013): Internet Banking benefit and challenges In An Emerging Economy, International Journal of Research in Business Management (IJRBM), Vol.1, Issue 1, 19-26.

6. Rupinder Pal Kaur (2013) Statistics of Cyber Crime in India: An Overview, International Journal of Engineering and Computer Science, Vol.2, Issue 8.

7. Muthukumaran.B (2008), "cybercrime scenario in India", criminal investigation department Review, pp.17-23.

8. Kumar.A (2002), "Cybercrime without punishment" available at unpanl.un.org.

9. Mulherkar, J (2006) how to escape phishing in online banking, 2006.

10. Umashankar Sivasubramanniam V. ICICI bank 2008, Tamil Nadu

11. Article on one in the three cyber attacks in banks are successful by Riju Mehta, 2017,economics time.

12. Alaganandam, H. , Mittal P. ,Singh, A., & Fleizach, C., 2007 Cybercriminal Activity.

13. Muthukumaran. B 2008. Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23.

14. Wall, D. 2001. 1 Cybercrimes and the Internet. Crime and the Internet: 1.

15. Ajjeet Singh Poonia, cybercrime, challenges and its classification, International journal of Emerging Trends and Technology in Computer Science (Volume 3, issue 6, 2014 pp-120).

16. Kamini Dashora, Cyber Crime in the society: Problem and Preventions, 2011, Vol-3, pp-243-244.

17. Cashell, B., Jackson, W.D., Jickling , M., & Webel, B. (2004). The economic impact of cyber-attacks, CRS Report for Congress. Congressional Research Service, The Liberary of Congress, 1-41.

18. Choo K.R. (2009). High tech criminal threats to the national information infrastructure. *Information Security Technical Report*, XXX, 1-8.

19. Manisha M. more and Nalawade, K.M. (2014): Cyber Crimes and Attacks: The Current Scenario. 1st National Conference Organization by NESGIO.

20. Soni RR and Soni Neena , An Investigation Study of banking Cyber Frauds with Special Reference to Private and Public banks, Vol. 2, 2(7), 22-27, (2013), Research Journal of Management

21. Kaul,Lokesh, (2009) Methodology of education research, Fauth revised enlarged edition, Vikas Publishing House Pvt. Ltd. Noida.

22. Best J., W. Kahn (2011) Research in education tenth edition entice hall of India, New Delhi.

23. Magal S.K. (2013), Statistics in and education second edition PHI Learning Private Limited, Delhi

24. Rehman Anisur SK (2016) "Use of E-Journal by the research scholar and faculty members in Geography subject in Aligarh Muslim University" – Vidyawarta International Multilingual Research Journal, issue 13, Vol. 6, 2016.

25. Rastogi Anita and Bibata Parashar (2009) "Effectives of cyber awareness in learning concept and teaching skill", Indian Journal of Teacher Education Anweshika, Vol. 6, Number- II, 2009.

26. United Nation Draft (2013), Comprehensive study on cybercrimes, United Nation's Office on Drug and Crime Vienna, 2013 Retrieved from: http://www.un.org/en/index.html .

27. Crime in India 2011 – Compendium (2012), National Crime Record Bureau, Ministry of Home Affairs, Government of India, New Delhi India Retrieved from: http://www.helplinelaw.com/1/CCII/cyber-crime-in-india-what-is-types-web-hijacking-cyber-stalking.html .

28. Ngpal, Rohas, Introduction to Indian Cyber Law (2008) , new world publication, Pune, India.

29. Suri, K.K. and Chhabra, T.N., Cybercrime (2003), Pentagon Press, New Delhi, India.

30. Seth, Karnika, "Evolving strategies for enforcement of cyber Law", Huffpost publications, New Delhi, 2010

31. National Crime Record Bureau (NCRB), Report 10, 2013 Retrieved form: http://ncrb.nic.in/ .

32. Sahu, Bhanu, " Identify Uncertainty of Cyber Crime and Cyber Laws", 2013 International Conference on Communication Systems and Network Technologies. Retrieved from: http://www.business-standard.com/article/pti-stories/30-of-indian-school-kids-in-some-states-faced-cyber-crime-114111000294_1.html .