## RESEARCH PROJECT REPORT ON

# “Cyber Crime in Banking Sector and Its Prevention”

Towards the partial fulfilment of Bachelor of Business Administration.

Rashtrasant Tukadoji Maharaj Nagpur University (RTMNU)

Guided by
**Mr. Aniruddha Akarte**

**Submitted by**
**Shivanshmani Tripathi**
**(6th SEMESTER)**

**Session 2021-2022**

G.S COLLEGE OF COMMERCE & ECONOMICS

# Certificate

This is to certify that the project entitled **“Cyber Crime in Banking Sector and Its Prevention”** has been submitted by Shivanshmani Tripathi , a student of Sixth semester B.B.A. This has not been submitted for any other examination and does not form a part of any other course undergoes by the candidate.

It is certified that he has ingeniously completed his project as prescribed by Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur.

| | |
|---|---|
| **Project Guide** | **Project Incharge** |
| ***Mr. Aniruddha Akarte*** | **Dr. Sonali Gadekar** |

# ACKNOWLEDGEMENT

This is to express my earnest gratitude and extreme joy at being bestowed with an opportunity to get an interesting and informative project on “Cyber Crime In Banking Sector and Its Prevention”

I have put in efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like extent my sincere thanks to all of them. I am extremely grateful to my project guide **Mr. Aniruddha Akarte** who has given an opportunity to work on such an interesting project. He proved to be a constant source of inspiration to me and provided constructive comments on how to make this report better.

I would like to express my gratitude towards my family members for their kind co-operation and encouragement which helped me in the completion of this project.

Credit also goes to my friends whose constant encouragement kept me in good stead. Lastly without fail I would thank all my faculties for providing all explicit and implicit support to me during the course of my project.

# DECLARATION

I here-by declare that the project with the title A study of consumer behavior towards **"Cyber Crime in Banking Sector and Its Prevention"** have been done by me in partial fulfillment of Bachelor of Businesss Administration Degree Examination as prescribed by Rashtrasant Tukadoji Maharaj Nagpur University and this has not been submitted for any other examination and does not form the part of any other course undertaken by me.

Date:

Name of the Student: Shivanshmani Tripathi

Place: Nagpur

SEM VI, BBA

# EXECUTIVE SUMMARY

The banking industry has enjoyed the ride of emerging technology to undergo significant changes. Banks are among the biggest beneficiaries of the IT revolution and have largely adopted Information Technology solutions for rendering the banking services to their customers. The proliferation in online transactions mounting on technologies like NEFT (National Electronic Fund Transfer), RTGS (Real-time Gross Settlement Systems), ECS (Electronic Clearing Service) and mobile transactions is a glimpse of the deep rooted technology in banking and financial matters. With the swift expansion of computer and internet technologies, new forms of worldwide crimes known as "Cyber Crimes" has evolved in the scene. Over a period of time, the nature and pattern of Cyber Crime incidents have become more sophisticated and complex. Banks and Financial Institutions remain the unabated targets of cyber criminals in the last decade. Notably financial gain is still one of the major motivations behind most cybercriminal activities and there is little chance of this changing in the near future.

This project focuses on the technical aspects of various types of cybercrimes concerning the banking and financial sector and their related impacts. Additionally, it identifies the threat vectors supporting these cybercrimes and develops measures to aid in the combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security.

# .TABLE OF CONTENTS

# 1. Introduction

The world is fast moving online with 46.1% of total world population now connected to the web according to internetlivestats.com (as on July 1, 2016). A remarkable instance of this phenomena has been experienced in India with a notable increase in the past three years i.e. 18% of the Indian population online in 2014, 27% in 2015 and 34.8% in 2016 (as on July 1, 2016). Today activities performed over the internet are not just limited to technology freaks for technical uses, rather every second individual is enjoying the easy internet availability and accessibility for day-to-day purposes like banking, ecommerce, education, entertainment and many more. Markedly, the wave of smartphones has definitely acted as a catalyst to this tremendous internet growth.

## Meaning of the Term “Cyber Crime”

As an increasing number of users are demanding online services, the background mission of providing balanced security and convenience is seeming to be a tough challenge due to numerous obtrusive actors collectively referred to as “Cyber-Crime”. Simply stated, “Cyber-Crime” is crime that involves a computer and a network (Moore R, 2005). Cyber-Crime is being considered a serious threat to all the aspects of a nation’s economic growth as maximum instances of the same are being observed in financial institutions. Cyber-Crime incidents include but are not limited to credit card fraud, spamming, spoofing, e-money laundering, ATM fraud, phishing, vishing, identity theft and denial of service.

Until mid-1990s, managing an account segment in many parts of the world was basic and dependable; anyway since the coming of innovation, the keeping

Money division saw a change in perspective in the wonder. Banks so as to upgrade their client base presented numerous stages. Through which exchanges should be possible absent much exertion. These advancements empowered the client to get to their bank funds 24*7 and year around through, ATMs and Web based managing an account methods.

Nonetheless, with the upgrade in innovation, keeping money cheats have additionally expanded similarly. Digital offenders are utilizing diverse intends to take ones bank data and at last their cash also.

It is in this manner, an aggregate agreement of banks and controllers to make arrangements and embrace measures so as to shield saving money stages from digital dangers. Various specialized guard and control estimates like expanded continuous supervision on exchanges have been attempted by the banks, nonetheless, even today the issue holds on. The explanation for this is the resistance measures right now accessible with banks are regularly receptive, tedious and accessible out in the open area which can be gotten to even by the digital criminal who thus receives measures to battle from these safeguards. The assailants allot their time in growing new methods for digital wrongdoing and furthermore at the same time take a shot at finding the answers for extension these protection measures.

One of the approaches to relieve the issue of digital wrongdoings in keeping money segment is to distinguish the variables identified with banks that are by and large focuses of such digital assaults, and why a few banks have never confronted such a circumstance. Banks which are for the most part focuses of digital wrongdoings experience the ill effects of different malware assaults in type of web based phishing, keystroke-loggings malwares, wholesale fraud, and so forth.

## 2. Cyber Crime in Banking Sector

Digital Wrongdoing can be just expressed as violations that include the utilization of PC and a network1 as a medium, source, instrument, target, or place of a wrongdoing. With the developing part of web based business and e- exchanges, the financial wrongdoing has floated towards the advanced world. Digital wrongdoings are expanding all around and India also has been seeing a sharp increment in digital violations related cases in the ongoing years.

In 2016, an investigation by Juniper Exploration evaluated that the worldwide expenses of cybercrime could be as high as 2.1 trillion by 2019.2 Anyway such gauges are just characteristic and the real expense of cybercrime including unreported harms is incalculable.

Digital Violations can be comprehensively arranged into classifications, for example, digital fear based oppression, Digital harassing, PC Vandalism, Programming Robbery, Wholesale fraud, Online Robberies and Fakes, Email Spam and Phishing and some more.

Nonetheless, from the part of money related digital wrongdoings submitted electronically, the accompanying classifications are transcendent:

- **Backdoor:** Backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, back doors are often used by attackers who detect and/or install it themselves. Whether installed as an administrative tool or a means of attack; a back door poses as a security risk aiding crackers looking for vulnerable systems. Once the backdoor has been established by cyber criminals, they gain system entry giving them complete access to all kind of sensitive information of the victim such as his financial details, account numbers, passwords etc. Such access enables the criminal to maliciously vandalize, alter, move, or delete files from the infected computer.

- Hacking: It is a system to increase unlawful access to a PC or system so as to take, degenerate, or misguidedly see information.

- Phishing: It is a procedure to acquire private data, for example, usernames, passwords, and charge/Master card subtleties, by imitating as a reliable substance in an electronic correspondence and replay similar subtleties for pernicious reasons.

- Vishing: It is the criminal routine with regards to utilizing social designing via phone framework to access private individual and budgetary data from the general population with the end goal of monetary reward. With the growth of mobile banking and the ability to conduct financial transactions online, vishing attacks have become even more attractive and lucrative for cyber criminals. It is the telephone equivalent of phishing. The term is a combination of "voice" and phishing. Vishing is the criminal act of using voice email, VoIP (voice over Internet Protocol), landline or cellular telephone to gain access to private, personal and financial information from the public for the purpose of financial reward by committing identity theft. It is typically used to steal credit card numbers by a scammer who usually pretends to be in legitimate business, and fools the victim into thinking he or she will profit. Vishing is very hard for legal authorities to monitor or trace. Thus it is onto the consumers to protect themselves, by being highly suspicious when receiving messages directing them to call and provide credit card or bank numbers. When in doubt, calling a company's telephone number listed on billing statements or other official sources is recommended instead of calling numbers from messages of dubious authenticity.

- E-mail Satirizing: It is a procedure of concealing an email's real starting point by fashioned the email header to seem to begin from one real source rather than the real beginning source.
- Spamming: A spambot is an automated computer program designed to send unsolicited bulk messages indiscriminately. They harvest e-mail addresses from material found on the Internet by automatically "crawling" the web, newsgroups, chat rooms, instant messengers and other contact databases to locate any and every email address they can find in order to build mailing lists for sending these e-mail, also known as spam. whereas some spambots can crack passwords and send spam using other people's accounts.
- Denial of Administration: This assault is described by an express endeavor by aggressors to forestall real clients of an administration from utilizing that benefit by "flooding" a system to forbid real system traffic, upset associations between two machines to deny access to an Administration or keep a specific individual from getting to an administration
- Advanced Constant Danger: It is portrayed as a lot of intricate, covered up and progressing PC hacking forms, frequently focusing on an explicit element to break into a system by keeping away from location together delicate data over a critical timeframe. The assailant generally utilizes some kind of social designing, to access the focused on system through authentic methods.
- ATM Skimming and Purpose of Offer Wrongdoings: It is a method of trading off the ATM machine or POS frameworks by introducing a skimming gadget on the machine keypad to show up as a veritable keypad or a gadget made to be fastened to the card peruser to resemble a piece of the machine. Furthermore, malware that takes Visa information specifically can likewise be introduced on these gadgets. Effective execution of skimmers cause in ATM machine to gather card numbers and individual distinguishing proof number (Stick) codes that are later repeated to complete fake exchanges.

# 3. Internet Banking in India

Electronic Keeping money or e-managing an account alludes to a framework where saving money exercises are completed utilizing instructive and PC innovation over human asset. In contrast with customary saving money administrations, in e-managing an account there is no physical association between the bank and the clients. E-managing an account is the conveyance of bank's data and administrations by banks to clients by means of various conveyance stages that can be utilized with various terminal gadgets, for example, PC and a cell phone with program or work area programming, phone or advanced TV.

The main activity in the territory of bank computerization was stemmed out of two progressive Boards on Computerization (Rangarajan Panel).6 The primary board of trustees was set up in 1984 which drew the outline for the automation and computerization in managing an account industry. The second Board of trustees was set up in 1989 which made ready for incorporated utilization of broadcast communications and PCs for applying completely the innovative leaps forward to the managing an account tasks. The center moved from the utilization of Cutting edge Record Posting Machines (ALPMs) for constrained computerization to full computerization at branches and to combination of the branches.7 Till 1989, banks in India had 4776 ALPMs at the branch level, more than 2000 software engineers/frameworks staff and more than 12000 Information Passage Terminal Administrators.

The RBI established a Working Gathering on web Managing an account. In light of the idea of access to the managing an account items and administrations, the gathering partitioned web keeping money into three frameworks.

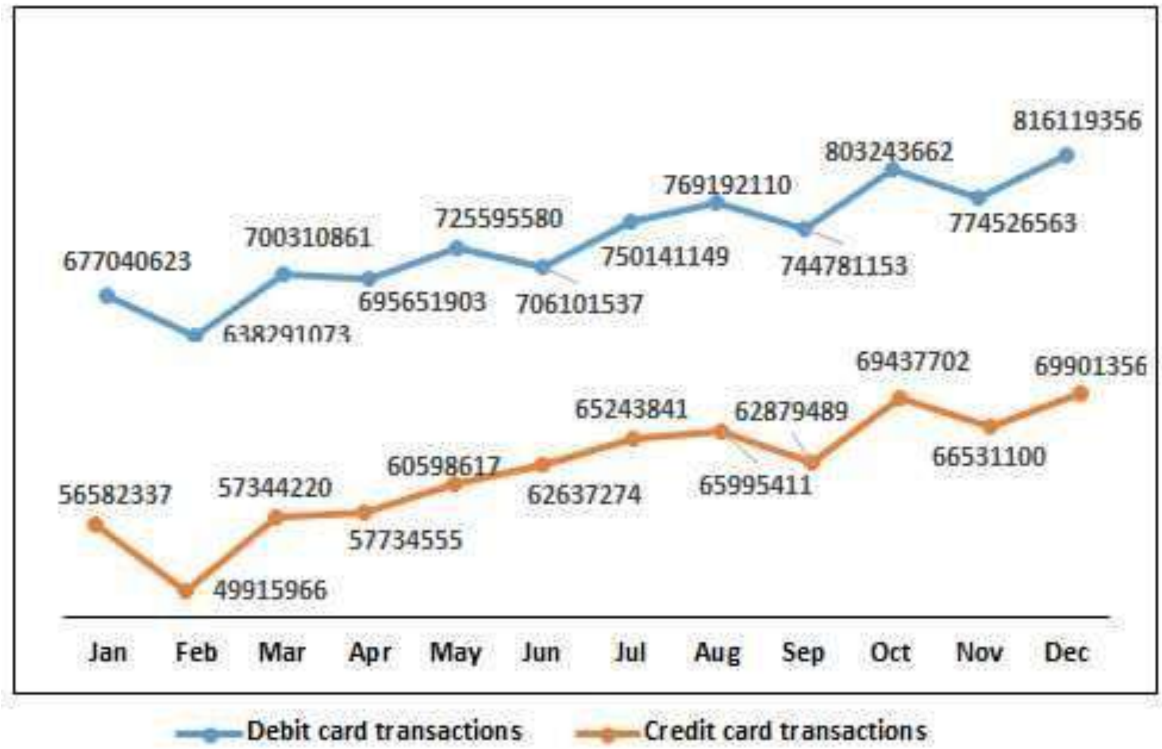
1) Enlightening Framework This framework expects banks to give data about financing costs, credit plans, branch areas and so on to the clients. Clients can download different kinds of utilization according to the necessities. Additionally clients are not required to uncover their personality and there is no sensible possibility of any unapproved individual getting into the creation arrangement of the bank.

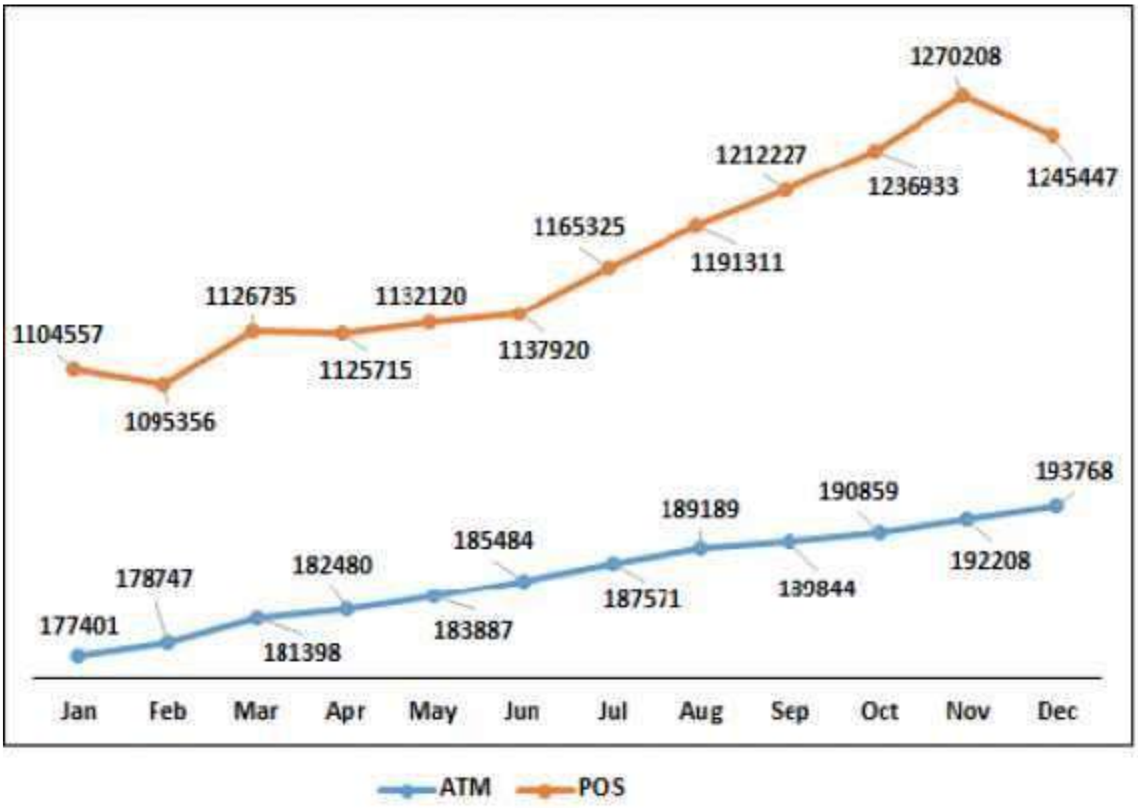
2) Open Framework This framework gives data to the client about his record balance, exchange subtleties and so on. The clients can look for the data after confirmation and signing in through the passwords.11

3) Value-based Framework In this framework a bank enables its clients to embrace exchanges through its framework and they are straightforwardly transferred to the client's record. There is bi-directional exchange that happens between the bank and the client and between the client and the outsider. This framework is anchored through security instruments like http and https. E- keeping money is otherwise called Digital Saving money, Home Saving money and Virtual Saving money. E-keeping money incorporates Web Saving money, Portable Managing an account, RTGS, ATMs, Mastercards, Charge cards, and Keen Cards and so forth.

A firm progression in the mounting paper less transactions numbers where a total of 9545797438 transactions were commenced using credit and debit cards in the year 2018 alone (Fig 1) can be partially accredited to the recent developments in the e-banking and e-commerce verticals.

In order to provide improved support for cashless transactions, a steady increase in the number ATM and POS machines is inevitable. Fig 2 highlights the growth in the number of ATM machines and POS machines installed across India in 2018.


816119356
803243662
769192110
725595580
700310861
677040623
774526563
750141149
744781153
695651903
706101537
638291073
69437702
69901356
65243841
62879489
60598617
66531100
56582337
57344220
62637274
65995411
57734555
49915966
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Debit card transactions
Credit card transactions


1270208
1212227
1236933
1245447
1165325
1191311
1126735
1132120
1104557
1125715
1137920
1095356
193768
190859
189189
192208
185484
139844
182480
187571
178747
183887
177401
181398
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
ATM
POS

# 4. Objective

1. **To identify the cybercrimes that affects the study area.**
2. **To examine the problems faced by banks in managing the cybercrimes and**
3. **To offer suggestions for the betterment of the study units.**
4. **Reasons for Cyber Crime**
5. **Impact of Cyber Crime on Banking Sector**

## 4.1. Reasons for Cyber Crime

Hart in his work, "the idea of law" has said 'people are helpless so standard of law is required to ensure them'. Applying this to the internet we may state that PCs are powerless so standard of law is required to secure and protect them against digital wrongdoing. The followings are a few reasons,

1) Capacity to store information in nearly little space
2) Easy to access
3) Complex
4) Negligence
5) Loss of proof

## 4.2. Impact of Cyber Crime on Banking Sector

The cases identified with cybercrimes have become savagely because of the upsurge in cell phones with web availability. Cell phones are these days utilized for various online exercises like web saving money, web based shopping, paying service charges and are continually according to the culprits to acquire access to private data.

Among the different inspirations for perpetrating a cybercrime, Monetary profit remains the consistent victor for the past numerous years surpassing different thought processes including requital, coercion and political causes.

Alarmingly, simple phishing attacks enjoy a success rate of 45% due to lack of awareness regarding the common safeguards to protect against the shrewd cyber criminals. The span of cybercrime can be estimated from the figures of 3855 cybercrimes committed for financial gain (NTRO) and 534 phishing incidents (CERT-In) in year 2015. These incidents only correspond to the reported incidents and do not comprise the incidents that went unreported and/or unnoticed.

Banks across the globe are increasing becoming prime targets of distributed denial-of-service (DDoS) attacks launched sometimes as a part of the plan to distract the security professional‟s attention to the depleting resources, while carrying out some additional dangerous activity in parallel like insertion of malware, or tampering with the IT assets. Such an embedded hacking campaign with a hidden agenda is usually referred to as Advanced Persistent Threat and is the latest kid on the board with enhanced complexity and shrewdness. In the cases, where the attackers are not able to yield some valuable information, they deface the banks website as a measure to take revenge against their failed attempts.

Besides the resulting financial gains from successful cyber attacks. the presence of online black markets commonly referred to as the „Darkweb‟[5]adds to the motivation of committing cybercrimes as a commonplace for exchanging personal information, latest exploits and sophisticated hacking kits. Sensitive information including stolen/leaked credit card numbers, online banking accounts, medical records and administrative access to servers are traded for money in these online fraud communities.

Amongst the various motivations for committing a cybercrime, Financial Gain remains the constant winner for the past many years overtaking other motives including revenge, extortion and political causes. (Fig 3)

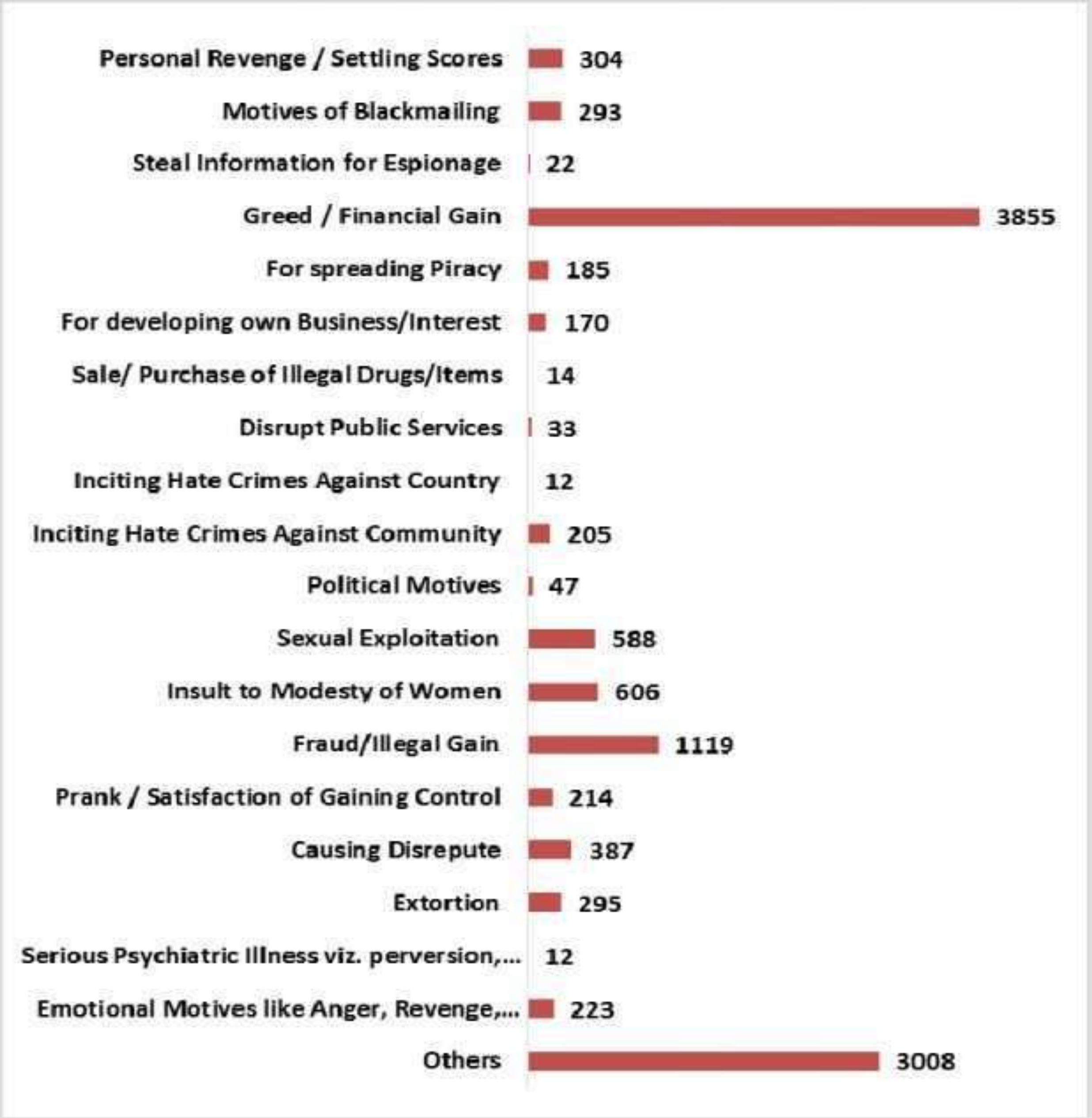


**Fig: 4.2. Impact of Cyber Crime on Banking Sector**

## 4.3. Safeguarding The Internet Banking Sector

Financial organizations in today"s date require well laid cyber security teams with distinguished digital leaders. According to PWC"s year"s global economic crime survey, 2016, too many organisations are leaving first response to their IT teams without adequate intervention or support from senior management and other key players. Specialized security teams with an upbeat mix of competent professionals should be employed to take a proactive stance when it comes to cybersecurity and privacy Organizations in the BFSI sector need to undergo rigorous and continuous cybercrime risk assessments to precisely assess, identify and improve their present security posture by viewing the organization"s policies from an attacker"s perspective and thusfacilitate enhanced security, operations, organizational management. Additionally, as long-term planning, cyber awareness need to introduced at a fundamental level in educational institutions with specialized security courses at graduate level to provide hands-on training on the latest attack methodologies and mitigation techniques using concepts like virtual cyber labs. A comprehensive threat intelligence technology is essential to foster organized and analysed threat information about potential or current attacks from the organization"s perspective. Alongside, threat intelligence helps organizations in understanding the common threat actors including latest vulnerabilities, exploits and advanced persistent threats (APTs) campaigns. On a national level, there is an urgent necessityof building capabilityof inspecting critical infrastructure in critical industry sectors before these are deployed in production to avoid any malicious intruders by leveraging the trusted hardware/software. Finally cooperation amongst Indian government sector and industrial groups is bound to strengthen the legal framework for cybersecurity with each blending in a different array of cyber risks and preventive mechanisms.

# 5. Hypothesis

1. There is no significant difference between a nature of bank and challenges faced by the banks for prevention of fraud.

2. There is no significant relationship between gender and opinion of the bankers regarding Online banking which is better substitute for Traditional banking.

# 6. Case Study

## 6.1. Case Study: India’s First Atm Card Fraud

The Chennai city police have busted a universal posse associated with digital wrongdoing, with the capture of Deepak prem manwani (22), who was caught in the act while breaking into an ATM in the city in June last, it is dependably learnt. The elements of the city cops' accomplishment can be ganged from the way that they have gotten a man who is on the needed rundown of the considerable FBI of the US. At the season of his detainment, he has with him Rs
7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Preceding that, he has left with Rs 50,000 from an ATM in Mumbai.

While researching Manwani's case, the police discover a digital wrongdoing including scores of people over the globe.

Manwani is a MBA drop-out from a pune school and filled in as a promoting official in a Chennai-based firm for quite a while.

Strikingly, his daring wrongdoing profession began in a web bistro. While perusing the net one day, he got pulled in to a sire which offered him help with breaking into the ATMs.

His contacts, sitting some place in Europe, were prepared to give him charge card number of a couple of American banks for $5 per code. This site likewise offered the attractive codes of those cards, however charged $200 per code. The administrator of the site has concocted an interesting plan to get the individual ID number (Stick) of the card clients. They skimmed another site which looked like that of a presumed telecom organizations.

That organization has a huge number of supporters. The phony site offered the guests to return $11.75 per head which, the site advertisers stated, has been gathered in overabundance unintentionally from them. Trusting that it was an authentic offer the telecom organization being referred to, a few lakh supporters signed on to the site to get back that minimal expenditure, yet in the process separated with their PINs.

Outfitted with every single essential datum to hack the bank ATMs, the posse began its orderly plundering. Evidently, manwani and numerous others of his kind went into an arrangement with the pack behind the site and could buy any measure of information, obviously on specific terms, or basically go into an arrangement on a goods sharing premise.

In the interim, manwani additionally figured out how to create 30 plastic cards that contained important information to empower him to break into ATMs.

He was enterprising to the point that he had the capacity to offer away a couple of such cards to his contacts in Mumbai. The police are vigilant for those people as well.

On receipt of huge scale protestations from the charged Visa clients and bank in the US, the FEI began an examination concerning the undertaking and furthermore alarmed the CBI in New Delhi that the universal pack has built up a few connections in India as well.

Manwani has since been developed safeguard after cross examination by the CBI. In any case, the city police trust this is the start of the finish of a noteworthy digital wrongdoing.

# 7. Findings

Greater part of the cybercrimes in this segment have come about out of hacking and data fraud.

- Banks are being focused again and again on the grounds that every one of the stores as money are held with the banks.
- The security of the clients is at a colossal hazard since it has turned out to be anything but difficult to hack their own subtleties.
- The product utilized for recognizing fakes as a rule is either obsolete or extremely tedious.
- The quantity of cases fathomed by the digital cell has remained reliably low throughout the previous four years, with just 20 percent achievement rate.

There is no explicit order that bargains with these violations, specifically with the Saving money Segments.

# 8. Suggestions

1) As there is no explicit requirement identified with the law, the significant effect of these violations is left unsolved numerous multiple times, a demonstration must be authorized to control this sort of danger.

2) The law implementation ought to be extremely unbending, and refreshed occasionally to monitor such wrongdoings.

3) There ought to be quick track portable courts to explain these cases, to meet the complaints and fabricate certainty among the general population.

4) The legislature ought to likewise keep a track on the working system exercises with the assistance of Huge Information Banks.

5) Disciplines and punishments should be practiced completely so as to limit the effect of these issues and punish the assailants.

6) Mindfulness Projects ought to be started so as to educate the general population about the continuous situation and forthcoming dangers.

7) General society should report these cases to the Digital Wrongdoing Branch in the issues related as opposed to simply alluding it to the banks, to guarantee quick and strict activities.

# 9. International Scenario

Cybercrime is "international" or "transnational" – there are ‘no cyber-borders between countries'.[2] International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. No matter, in developing or developed countries, governments and industries have gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale. China–United States cooperation is one of the most striking progress recently, because they are the top two source countries of cybercrime.

Information and communication technology (ICT) plays an important role in helping ensure interoperability and security based on global standards. General countermeasures have been adopted in cracking down cybercrime, such as legal measures in perfecting legislation and technical measures in tracking down crimes over the network, Internet content control, using public or private proxy and computer forensics, encryption and plausible deniability, etc.[2] Due to the heterogeneity of law enforcement and technical countermeasures of different countries, this article will mainly focus on legislative and regulatory initiatives of international cooperation.

## Typology

In terms of cybercrime, we may often associate it with various forms of Internet attacks, such as hacking, Trojans, malware (keyloggers), botnet, Denial-of-Service (DoS), spoofing, phishing, and vishing. Though cybercrime encompasses a broad range of illegal activities, it can be generally divided into five categories:

## Intrusive Offences

Illegal Access: "Hacking" is one of the major forms of offences that refers to unlawful access to a computer system.

Data Espionage: Offenders can intercept communications between users (such as e-mails) by targeting communication infrastructure such as fixed lines or wireless, and any Internet service (e.g., e-mail servers, chat or VoIP communications).

Data Interference: Offenders can violate the integrity of data and interfere with them by deleting, suppressing, or altering data and restricting access to them.

## Content-related offences

Pornographic Material (Child-Pornography): Sexually related content was among the first content to be commercially distributed over the Internet.

Racism, Hate Speech, Glorification of Violence: Radical groups use mass communication systems such as the Internet to spread propaganda.

**Religious Offences**: A growing number of websites present material that is in some countries covered by provisions related to religious offences, e.g., anti-religious written statements.

Spam: Offenders send out bulk mails by unidentified source and the mail server often contains useless advertisements and pictures.

## Copyright and trademark-related offences

Common copyright offences: cyber copyright infringement of software, music or films.

Trademark violations: A well-known aspect of global trade. The most serious offences include phishing and domain or name-related offences, such as cybersquatting.

## Computer-related offences

Fraud: online auction fraud, advance fee fraud, credit card fraud, Internet banking

Forgery: manipulation of digital documents.

Identity theft: It refers to stealing private information including Social Security Numbers (SSN), passport numbers, Date of birth, addresses, phone numbers, and passwords for non-financial and financial accounts.

## Combination offences

Cyberterrorism: The main purposes of it are propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, terrorist financing and attacks against critical infrastructure.

Cyberwarfare: It describes the use of ICTs in conducting warfare using the Internet.

Cyberlaundering: Conducting crime through the use of virtual currencies, online casinos etc.

## Threats

Similar to conventional crime, economic benefits, power, revenge, adventure, ideology and lust are the core driving forces of cybercrime. Major threats caused by those motivations can be categorized as following:

Economic security, reputation and social trust are severely challenged by cyber fraud, counterfeiting, impersonation and concealment of identity, extortion, electronic money laundering, copyright infringement and tax evasion.

Public interest and national security is threatened by dissemination of offensive material —e.g., pornographic, defamatory or inflammatory/intrusive communication— cyber stalking/harassment, Child pornography and paedophilia, electronic vandalism/terrorism.

Privacy, domestic and even diplomatic information security are harmed by unauthorized access and misuse of ICT, denial of services, and illegal interception of communication.

Domestic, as well as international security are threatened by cybercrime due to its transnational characteristic. No single country can really handle this big issue on their own. It is imperative for us to collaborate and defend cybercrime on a global scale.

## International trends

As more and more criminals are aware of potentially large economic gains that can be achieved with cybercrime, they tend to switch from simple adventure and vandalism to more targeted attacks, especially platforms where valuable information highly concentrates, such as computer, mobile devices and the Cloud. There are several emerging international trends of cybercrime.

Platform switch: Cybercrime is switching its battle ground from Windows- system PCs to other platforms, including mobile phones, tablet computers, and VoIP. Because a significant threshold in vulnerabilities has been reached. PC vendors are building better security into their products by providing faster updates, patches and user alert to potential flaws. Besides, global mobile devices' penetration—from smart phones to tablet PCs—accessing the Internet by 2013 will surpass 1 billion, creating more opportunities for cybercrime. The massively successful banking Trojan, Zeus is already being adapted for the mobile platform. Smishing, or SMS phishing, is another method cyber criminals are using to exploit mobile devices, which users download after falling prey to a social engineering ploy, is **designed** to defeat the SMS-based two-factor authentication most banks use to confirm online funds transfers by customers. VoIP systems are being used to support vishing (telephone-based phishing) schemes, which are now growing in popularity.

Social engineering scams: It refers to a non-technical kind of intrusion, in the form of e-mails or social networking chats, that relies heavily on human interaction and often involves fooling potential victims into downloading malware or leaking personal data. Social engineering is nevertheless highly effective for attacking well-protected computer systems with the exploitation of trust. Social networking becomes an increasingly important tool for cyber criminals to recruit money mules to assist their money laundering operations around the globe. Spammers are not only spoofing social networking messages to persuade targets to click on links in emails — they are taking advantage of users' trust of their social networking connections to attract new victims.

Highly targeted: The newest twist in "hypertargeting" is malware that is meant to disrupt industrial systems — such as the Stuxnet network worm, which exploits zero-day vulnerabilities in Microsoft. The first known copy of the worm was discovered in a plant in Germany. A subsequent variant led to a widespread global outbreak.

Dissemination and use of malware: malware generally takes the form of a virus, a worm, a Trojan horse, or spyware. In 2009, the majority of malware connects to host Web sites registered in the U.S.A. (51.4%), with China second (17.2%), and Spain third (15.7%). A primary means of malware dissemination is email. It is truly international in scope.

Intellectual property theft (IP theft): It is estimated that 90% of the software, DVDs, and CDs sold in some countries are counterfeit, and that the total global trade in counterfeit goods is more than $600 billion a year. In the USA alone, IP theft costs businesses an estimated $250 billion annually, and 750,000 jobs.

## International legislative responses and cooperation G8

Group of Eight (G8) is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.

In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.

## **United Nations**

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.[7]

## ITU

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cybersecurity issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS).

In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime.

In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society.

## **Council of Europe**

Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.

In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. [8] It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

## Regional responses

### APEC

Asia-Pacific Economic Cooperation (APEC) is an international forum that seeks to promote promoting open trade and practical economic cooperation in the Asia-Pacific Region. In 2002, APEC issued Cybersecurity Strategy which is included in the Shanghai Declaration. The strategy outlined six areas for co- operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education.

### OECD

The Organisation for Economic Co-operation and Development (OECD) is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade.

In 1990, the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council. In 2002, OECD announced the completion of "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security".

## European Union

The coat of arms of the European Cybercrime Centre

In 2001, the European Commission published a communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

In 2002, EU presented a proposal for a “Framework Decision on Attacks against Information Systems”. The Framework Decision takes note of Convention on Cybercrime, but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.

## Commonwealth

In 2002, the Commonwealth of Nations presented a model law on cybercrime that provides a legal framework to harmonise legislation within the Commonwealth and enable international cooperation. The model law was intentionally drafted in accordance with the Convention on Cybercrime.

## ECOWAS

The Economic Community of West African States (ECOWAS) is a regional group of west African Countries founded in 1975 it has fifteen member states. In 2009, ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law.

## GCC

In 2007, the Arab League and Gulf Cooperation Council (GCC) recommended at a conference seeking a joint approach that takes into consideration international standards.

## Voluntary industry response

During the past few years, public-private partnerships have emerged as a promising approach for tackling cybersecurity issues around the globe. Executive branch agencies (e.g., the Federal Trade Commission in US), regulatory agencies (e.g., Australian Communications and Media Authority), separate agencies (e.g., ENISA in the EU) and industry (e.g., MAAWG, …) are all involved in partnership.

In 2004, the London Action Plan was founded, which aims at promoting international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses.

## Case analysis

### U.S.

According to Sophos, the U.S. remains the top-spamming country and the source of about one-fifth of the world's spam. Since fighting cybercrime involves great amount of sophisticated legal and other measures, only milestones rather than full texts are provided here.

Legal and regulatory measures

The first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 (CFAA).

In 1986, Electronic Communications Privacy Act (ECPA) was an amendment to the federal wiretap law.

“National Infrastructure Protection Act of 1996”. “Cyberspace Electronic Security Act of 1999”. “Patriot Act of 2001”.

Digital Millennium Copyright Act (DMCA) was enacted in 1998. Cyber Security Enhancement Act (CSEA) was passed in 2002.

Can-spam law issued in 2003 and subsequent implementation measures were made by FCC and FTC.[9]

In 2005 the USA passed the Anti-Phishing Act which added two new crimes to the US Code.[10]

In 2009, the Obama Administration released Cybersecurity Report and policy. Cybersecurity Act of 2010, a bill seeking to increase collaboration between the public and the private sector on cybersecurity issues.[11]

A number of agencies have been set up in the U.S. to fight against cybercrime, including the FBI, National Infrastructure Protection Center, National White Collar Crime Center, Internet Fraud Complaint Center, Computer Crime and Intellectual Property Section of the Department of Justice (DoJ), Computer Hacking and Intellectual Property Unit of the DoJ, and Computer Emergency Readiness Team/Coordination Center (CERT/CC) at Carnegie-Mellon, and so on.

CyberSafe is a public service project designed to educate end users of the Internet about the critical need for personal computer security.

## Technical measures

Cloud computing: It can make infrastructures more resilient to attacks and functions as data backup as well. However, as the Cloud concentrates more and more sensitive data, it becomes increasingly attractive to cybercriminals.

Better encryption methods are developed to deal with phishing, smishing and other illegal data interception activities.

The Federal Bureau of Investigation has set up special technical units and developed Carnivore, a computer surveillance system which can intercept all packets that are sent to and from the ISP where it is installed, to assist in the investigation of cybercrime.

Industry collaboration

Public-private partnership: in 2006, the Internet Corporation for Assigned Names and Numbers (ICANN) signed an agreement with the United States Department of Commerce (United States Department of Commerce) that they partnered through the Multistakeholder Model of consultation.

In 2008, the second annual Cyber Storm conference was exercised, involving nine states, four foreign governments, 18 federal agencies and 40 private companies.

In 2010, National Cyber Security Alliance’s public awareness campaign was launched in partnership with the U.S. Department of Homeland Security, the Federal Trade Commission, and others.

Incentives for ISP: Though the cost of security measures increases, Internet Service Providers (ISP) are encouraged to fight against cybercrime to win consumer support, good reputation and brand image among consumer and peer ISP as well.

## International cooperation

USA has signed and also ratified Convention on Cybercrime.

United States has actively participated in G8/OECD/APEC/OAS/U.S.-China cooperation in cracking down international cyber crime.

Future challenges

Privacy in tracking down cybercrime is being challenged and becomes a controversial issue.

**Public-private partnership**.

As the U.S. government gets more involved in the development of IT products, many companies worry this may stifle their innovation, even undermining efforts to develop more secure technology products. New legislative proposals now being considered by the U.S. Congress could be potentially intrusive on private industry, which may prevent enterprises from responding effectively to emerging and changing threats. Cyber attacks and security breaches are increasing in frequency and sophistication, they are targeting organizations and individuals with malware and anonymization techniques that can evade current security controls. Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defense. Relatively few organizations have recognized organized cyber criminal networks, rather than hackers, as their greatest potential cyber security threat; even fewer are prepared to address this threat.

## China

In January 2009, China was ranked No.3 spam-producing country in the world, according to data compiled by security vendor Sophos. Sophos now ranks China as spam producer No.20, right behind Spain.

China's underground economy is booming with estimated 10 billion RMB in 2009. Hacking, malware and spam are immensely popular. With patriotic hacktivism, people hack to defend the country.

## Legal and regulatory measures

Criminal Law – the basic law identifies the law enforcement concerning cybercrime.

In 2000, the Decision on Internet Security of the Standing Committee of the NPC was passed.

In 2000, China issued a series of Internet rules that prohibit anyone to propagate pornography, virus and scams.

In 2003, China signed UN General Assembly Resolution 57/239 on “Creation of a global culture of cybersecurity”.

In 2003, China signed Geneva Declaration of Principles of the World Summit on the Information Society.

In 2006, an anti-spam initiative was launched.

In July 2006, the ASEAN Regional Forum (ARF), which included China, issued a statement that its members should implement cybercrime and cybersecurity laws “in accordance with their national conditions and by referring to relevant international instruments”.

In 2009, ASEAN-China framework agreement on network and information security emergency response were adopted.

## Technical measures

Internet censorship: China has made it tougher to register new Internet domains and has put on stricter content control to help reduce spam.

"Golden Shield Project" or "The Great Firewall of China": a national Internet control and censorship project. In 2009, Green Dam software: It restricts access to a secret list of sites, and monitors users'activity.

Operating system change: China is trying to get around this by using Linux, though with a lot of technical impediments to solve.

Industry collaboration

Internet Society of China — the group behind China's anti-spam effort — is working on standards and better ways of cooperating to fight cybercrime.

ISPs have become better at working with customers to cut down on the spam problem.

## International cooperation

In 2005, China signed up for the London Action Plan on spam, an international effort to curb the problem.

Anti-Spam "Beijing Declaration"2006 International Anti-Spam Summit was held.

The APEC Working Group on Telecommunications agreed an action plan for 2010–2015 that included "fostering a safe and trusted ICT environment".

In January 2011, the United States and China committed for the first time at head of state level to work together on a bilateral basis on issues of cybersecurity. "Fighting Spam to Build Trust" will be the first effort to help overcome the trust deficit between China and the United States on cybersecurity. Cyber Security China Summit 2011 will be held in Shanghai.

## Achievement and future challenges

Successfully cracking down spam volume in 2009. However, insufficient criminal laws and regulations are great impediments in fighting cybercrime. A lack of electronic evidence laws or regulations, low rank of existing internet control regulations and technological impediments altogether limit the efficiency of Chinese governments' law enforcement.

- **List of Top 10 Countries with the highest rate of Cybercrime (source: BusinessWeek/Symantec) :**

Each country lists 6 contributing factors, share of malicious computer activity, malicious code rank, spam zombies rank, phishing web site hosts rank, bot rank and attack origin, to substantiate its cybercrime ranking.

## Cybercrime Top 10 Countries -

### 1. United States of America

Share of malicious computer activity: 23% Malicious code rank: 1

Spam zombies rank: 3

Phishing web site hosts rank: 1 Bot rank: 2

Attack origin rank: 1

## 2. China

Share of malicious computer activity: 9% Malicious code rank: 2

Spam zombies rank: 4

Phishing web site hosts rank: 6 Bot rank: 1

Attack origin rank: 2

## 3. Germany

Share of malicious computer activity: 6% Malicious code rank: 12

Spam zombies rank: 2

Phishing web site hosts rank: 2 Bot rank: 4

Attack origin rank: 4

## 4. Britain

Share of malicious computer activity: 5% Malicious code rank: 4

Spam zombies rank: 10

Phishing web site hosts rank: 5 Bot rank: 9

Attack origin rank: 3

## 5. Brazil

Share of malicious computer activity: 4% Malicious code rank: 16

Spam zombies rank: 1

Phishing web site hosts rank: 16 Bot rank: 5

Attack origin rank: 9

## 6. Spain

Share of malicious computer activity: 4% Malicious code rank: 10

Spam zombies rank: 8

Phishing web site hosts rank: 13 Bot rank: 3

Attack origin rank: 6

## 7. Italy

Share of malicious computer activity: 3% Malicious code rank: 11

Spam zombies rank: 6

Phishing web site hosts rank: 14 Bot rank: 6

Attack origin rank: 8

## 8. France

Share of malicious computer activity: 3% Malicious code rank: 8

Spam zombies rank: 14

Phishing web site hosts rank: 9 Bot rank: 10

Attack origin rank: 12

## 9. Turkey

Share of malicious computer activity: 3% Malicious code rank: 15

Spam zombies rank: 5

Phishing web site hosts rank: 24 Bot rank: 8

Attack origin rank: 12

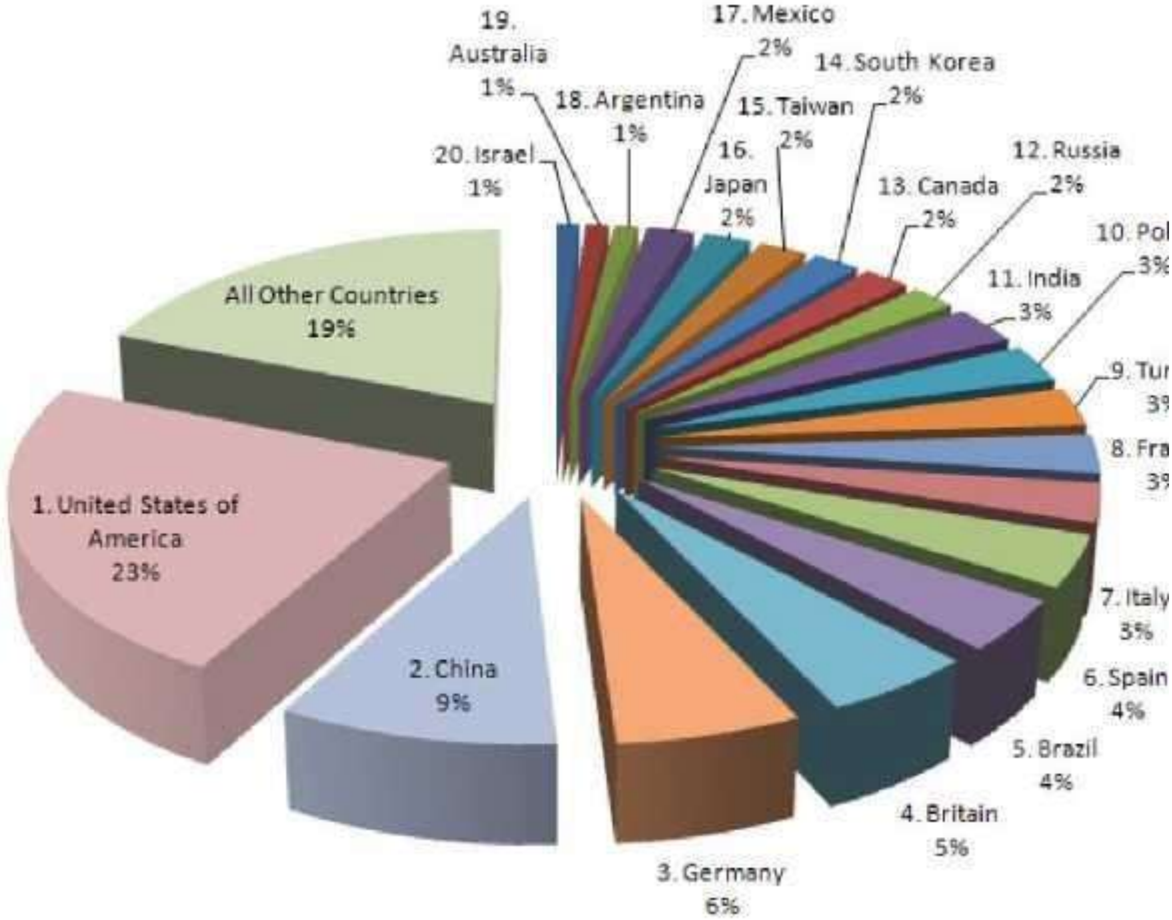
## 10. Poland

Share of malicious computer activity: 3% Malicious code rank: 23

Spam zombies rank: 9

Phishing web site hosts rank: 8 Bot rank: 7

Attack origin rank: 17



Cybercrime: Top 20 Countries

# 10. Conclusion

The investigation has given an outline to the idea of E-saving money by talking about profoundly different digital wrongdoings, distinguished explicitly in the managing an account division. The Saving money framework is the soul and spine of the economy. Data Innovation has turned into the foundation of the saving money framework. It gives an enormous help to the regularly expanding difficulties and managing an account necessities. By and by, banks can't consider presenting money related item without the nearness of Data Innovation. Anyway Data Innovation has an unfavorable effect too on our managing an account division where wrongdoings like, phishing, hacking, falsification, bamboozling and so on are submitted. There is a need to avert digital wrongdoing by guaranteeing validation, recognizable proof and check procedures when an individual goes into any sort of saving money exchange in electronic medium. The development in digital wrongdoing and intricacy of its examination strategy requires proper measures to be embraced. It is basic to expand the collaboration between the partners to handle digital wrongdoing. As indicated by National Wrongdoing Records Agency it was discovered that there has been a tremendous increment in the quantity of digital violations in India in recent years. Electronic wrongdoing is a difficult issue. In instances of digital wrongdoing, there isn't just money related misfortune to the banks yet the confidence of the client upon banks is additionally undermined. Indian managing an account division can't abstain from keeping money exercises helped out through electronic medium as the investigation recommend that there has been an expansion in the quantity of installments in e-saving money. Nonetheless, the adjustment in the saving money industry must be such which suits the Indian market. In conclusion, it very well may be presumed that to dispense with and kill cybercrime from the internet is certifiably not an apparently conceivable assignment however it is conceivable to have an ordinary keep an eye on managing an account exercise and exchange. The main auspicious advance is to make mindfulness among individuals about their rights and obligations and to additionally making the usage of the laws all the more firm and stringnent to check wrong doing.

.

# 11. Bibliography

**Websites :**

- **https://cybercrime.gov.in/**
- **https://en.m.wikipedia.org**
- **https://www.unodc.org/unodc/en/cybercrime**
- **https://leidenlawblog.nl/articles/cybercrime-and-cybersecurity-the-need-for-international-cybersecurity**
- **https://m.rbi.org.in/**
- **https://www.cybercrimejournal.com**
- **http://now-static.norton.com**

**Search Engines :**

- **www.google.com**
- **www.yahoo.com**
- **Wikipedia**

# 12. Questionnaire

1. Name:

2. Age :

3. Gender :

4. Educational qualification :

5. Organization :

6. Area of employment :

A. Software Design and Development [ ]

B. Hardware development

C. I.T.E.S. [ ]

D. B P O [ ]

E. Banks and Financial Institutions [ ]

F. Others (Specify)

7. Are you aware of "Information Technology' (IT) Act 2000 Yes [ ] No [ ]

8. Sec.43 ofthe I T Act provides penalty for damage to computer, computer systems etc., such as illegal access to computer systems, downloading or copying data, inducing virus attack on it, damaging the computer, its stored data or network etc shall be liable to pay by way of compensation up to Rs. 1 Crore. Do you think that this is:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

9. Sec.65 of the IT Act provides for punishment for ‘Tampering with computer source documents’ with imprisonment up to three years or with fine up to Rs.Two lakhs or with both. Do you think that this is:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

10. ‘Hacking’ is punishable under Sec. 66 of the IT Act with imprisonment up to3 years or with fine ofRs.Two lakhs, or with both. Do you think that this is:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

11. ‘Publishing ofinformation which is obscene in electronic form' under Sec. 67 of the IT Act with imprisonment up to 10 years or with fine of Rs.Two lakhs, or with both. Doyou think that this is:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

12. ‘Breach of confidentiality and privacy' under Sec. 72 of the IT Act with imprisonment up to 2 years or with fine ofRs. One lakh, or with both. In addition to this, it is proposed to amend this clause and bring about by way of compensation for breach of confidentiality; capturing or broadcasting an image of a person without consent, to a sum of Rs.25 Lakhs. Do you think that this is:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

13. As provided under Sec.85 ‘offences by companies’, all persons, who were in charge of, and were responsible to, the company for the conduct of business at the time of the breach of any provision of the I T Act shall be liable to be proceeded against and punished accordingly; with the exception of any one proving beyond reasonable doubt that the incident took place without his knowledge or that the had exercised “due Diligence” to prevent it. Do you agree with this clause?

Yes [ ] No [ ]

14. Sec.79 provides that ‘Network service providers not to be liable in certain cases', in instances where the service provider proves that the contravention was committed without his knowledge or that he had exercised all due diligence to prevent its commission. It is proposed to amend this limiting the liability of such intermediaries.

Do you agree to this?

Yes [ ] No [ ]

15. Do you think the IT Act 2000 is capable of preventing cyber Crime?

Yes [ ] No [ ]

16. Cyber crimes are committed beyond international boundaries. Do you think that an international law, rather than a law specific to a nation's jurisdiction is more beneficial to face future challenges such as international fraud, money laundering and terrorism?

Yes [ ] No [ ]

17. Do you think that some aspects of intellectual property right protection, trademark and copyright infringements should also be incorporated within IT Act?

Yes [ ] No [ ]

17-A. Which of these cyber crimes that are most frequently encountered by you?

A. E-mail bombing [ ]

B. Data diddling [ ]

C. Salami attacks [ ]

D. Virus/Worm Attacks [ ]

E. Logic bombs [ ]

F. Trojan attacks [ ]

G. Internet time thefts [ ]

H. Web jacking [ ]

18. Have come across any cyber crime during your occupation?

Yes [ ] No [ ]

19. If you come across a cyber crime in your line ofwork how would you respond to it?

A. Inform Superior personnel within the organization [ ]

B. Inform the Police [ ]

C. React to it on your own initiative [ ]

D. Ignore it [ ]

20. Does your organization have a specific protocol in preventing such instances?

Yes [ ] No [ ]

21. Should every organization have its own cyber security system?

Yes [ ] No [ ]

22. Should law alone particularly the government worry about cyber crime?

Yes [ ] No [ ]

23. Most of the cyber crime is by insiders or disgruntled ex- employees do you agree with this?

Yes [ ] No [ ]

24. Do you think that women and children are more prone to obscene cyber crimes?

Yes []    No [ ]

25. Do you opine that proper education in the use of cyberspace by women and children would prevent cyber crime to a certain extent?

Yes [ ]    No [ ]

26. The Department of Justice and the Information Technology Association of America (I T A A) has initiated a joint campaign to educate and raise awareness of responsibility among computer users. Do you think that India should have a similar campaign, particularly originating from Bangalore?

Yes [ ]    No [ ]