Suresh Gyan Vihar University,

Jaipur International Journal of Converging Technologies and Management (IJCTM)

Volume 1, Issue 2, 2015

ISSN : 2455-7528

Cyber crime Escalation Vs solutions: a Literature Snapshot

Dr. Raksha Chouhan

Internet based global fraud rate is increasing rapidly and there is a potential impact of cyber crime on quality production time, overhead cost, consumer trust, market value as well as on economy of the country. Internet has acted as an alternate avenue for the criminals to conduct their activities, and commence attacks with relative murkiness. In this age cybercriminals are tagrting the social and professional networks and threats are directed at the mobile platform like smartphones and tablets. The major cyber crimes reported in India are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber squatting, cyber stalking, phishing etc. The failure towards providing trusted secure services in modern computer network technologies has a remarkable socio-economic impact in global aspect and it is alerting us to claim attention in national capitals and dedicated legislation on cyber crime to supplement the Indian Penal Code. In this paper an analytical approach has been introduced from emergence of cyber crime to prevention strategies used for cyber crime. This paper throws light on status of cyber crime in current scenario, available solutions including steps taken by nongovernment and government organizations to avoid cyber crime and forthcoming challenges as well as upon National, International accordance and solutions to deal with the same.

KEYWORDS: Cyber Crime, Cyber Attacks and Piracy, Cyber Safety, Cyber Law, I.T. Act.

[*] Faculty, Prestige Institute of Management and Research, D.A.V.V. Indore (Madhya Pradesh)
E-mail: raksha_chauhan@pimrindore.ac.in

1. Introduction

Internet technology have not come up without drawbacks, although it make our life speedy but at the same time it requires lot of alertness also. Among E-frauds obscenity, defamation, forgery, criminal intimidation, slander have come up rapidly. Cybercrime deals with the crimes related to computer world. The cyber crime includes the crime in which computer is involved in some format. Cyber criminal is a person who commits an illegal act with a guilty intension or commits a crime. The cyber criminal may be a kids and teenagers between ages 9-17 years, organized hackers (pranksters) or crackers, professional hackers or career criminals, peeved employees, cyber terrorists, cyber bulls, salami attacker etc. Cybercrime damages trade, competitiveness, innovation, and global economic growth. In figure 1 percentage wise country confidence ranking regarding to current scenario of cyber tracking with their borders has been shown where: Australia (.08%),Brazil (.32%), Canada (.17%), China (.63%), European Union (.41%), France (.11%), Germany (1.60%), **India (.21%)**, Japan (.02%), Mexico (.17%), Russia (.10%), Saudi Arabia (.17%), Turkey (.07%), United Kingdom (.16%), United States (.64%), Argentina (n/a), Colombia (.14%), Indonesia (n/a), Ireland (.20%), Italy (.04%), Kenya (.01%), Korea (n/a), Malaysia (.18%), Netherlands (1.50%), New Zealand (.09%), Nigeria (.08%), Norway (.64%), Singapore (.41%), South Africa (.14%), United Arab Emirates (.11%), Vietnam (.13%), Zambia (.19%) [1]:

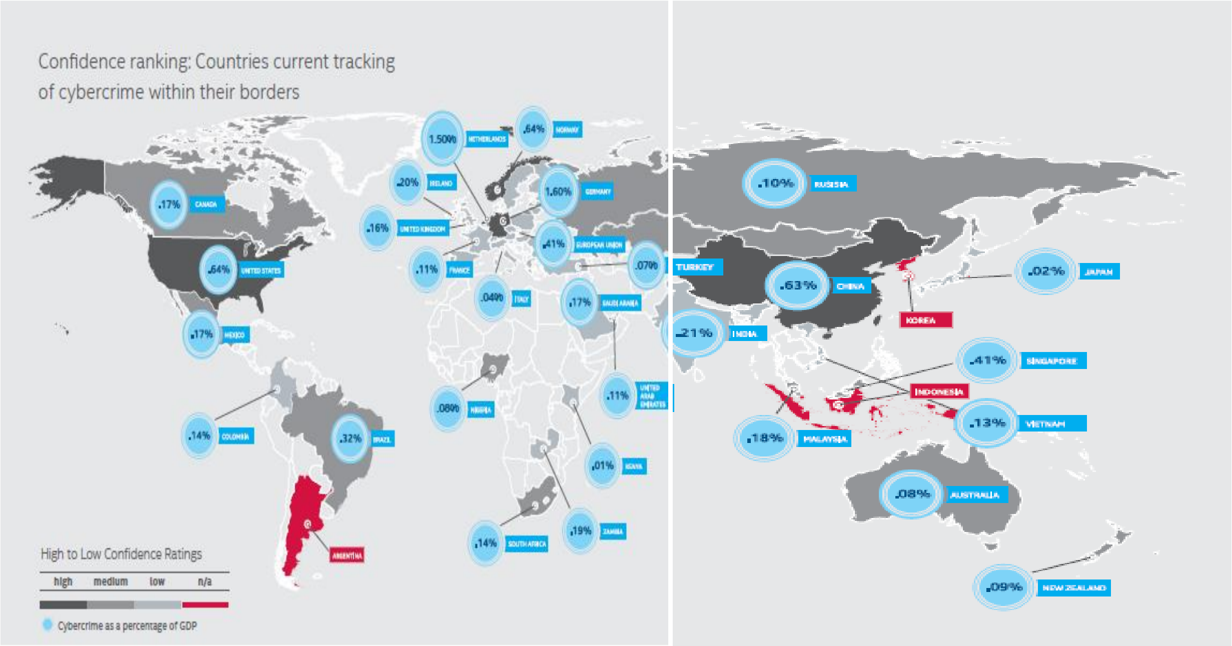
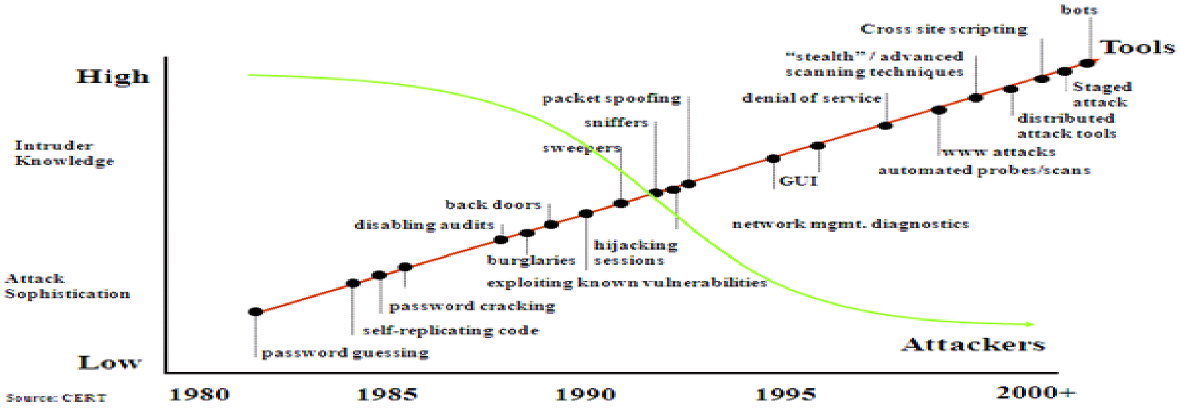


Fig 1: Confidence ranking in current scenario for cyber tracking

In pre 2000 cybercrime was considered as immature or childish behavior of criminal as a practical joke or game by those who committed it. Earlier it was centered on or around one-man operated crime with the intension to exploit the limitations in the computer operating system or computer network. In most cases these crimes were committed by those people who felt challenged to prove that they could beat the system without any intension of gaining financial benefit where a great deal of financial damage could actually result. At this time Criminal defense policies was also largely based on the fact that no real intentional damage was done and, in a large number of cases, the penalty for the crime was showing how the computer system had been hacked by the hacker. In post 2000 cyber criminal gangs had introduced a professional element into the world of cybercrime. They had organized and focused their attention towards profit gain and had developed tactics to making use of computer networks to infiltrate and take advantage of the trust of other users of that computer network for huge financial gain. They had worked out hardened and they had realized that the Internet was a safe domain, with much less risk, with which to operate and generate large profits [4]. Fig 2 is showing various stages of cyber attack evolution from year 1980 to the year 2000+ [3]:



Source: CERT

Fig 2: Various stages of cyber attack evolution

While the worldwide scenario on cyber crime looks desolate, the situation in India isn't any better. India in rated in the top 5 countries affected with cyber crimes and gaining momentum from simple email type of crime to serious crime like hacking, phishing, Vishing, source code theft, cyber staking, internet time theft, Web Jacking and cross site scripting etc. In table 1 cyber crime classification has been shown [2]:

S. No.	User based	Property based	Society based
1	Email spoofing	Intellectual property	Forgery
2	Cyber stalking	Computer wreckage	Financial Crimes
3	Cheating & fraud	Virus Transmitting	Child pornography
4	Unauthorized access	Unauthorized access	Trafficking
5	Defamation	online theft	Online gambling

Table 1: Cyber Crime Classification

2. Rationale and objectives of the Study

Information plays essential role for an individual, cooperate sector as well as for state and country. India has emerged as a favourite among cybercriminals, mostly hackers and other malicious users who use the internet to commit crimes and due to insufficient rules and regulations privacy of information is easily breached. According to Computer Emergency Response Team-India (CERT-In) report till May 2014 total 9, 9,174 Indian websites were hacked by hacker groups spread across the world [5]. According to an Assoc ham-Mahindra SSG study "The number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges" [6]. Objective of my study are:

1. The study is going to help in identifying different modes by which cybercrime has been spread across the world as well as significant variants which can be used to detect and prevent our society to combat with cybercrime.
2. To recognize emerging cyber safety mechanism and various initiatives taken by international and national organizations so that future direction can be traced towards the development of advanced methodologies.

3. Methodology

This study is descriptive in nature. An attempt has been made to analyze cyber crime report given by different media resources from theoretical and investigative points of views with sentencing research. The material has been referred from Online as well as desk based book reviews, articles, reports, research and conference papers. Thus a combination of existing literature studies and in-depth secondary database material is used to fulfill the objective.

4. Cyber Crime Variants

In the present scenario the online channels are facing tricky and globally-integrated technological crimes. An offence of cyber crime involves use of computer, internet, cyber space, tools and techniques of World Wide Web. Fig 3 illustrates cyber crime variants.

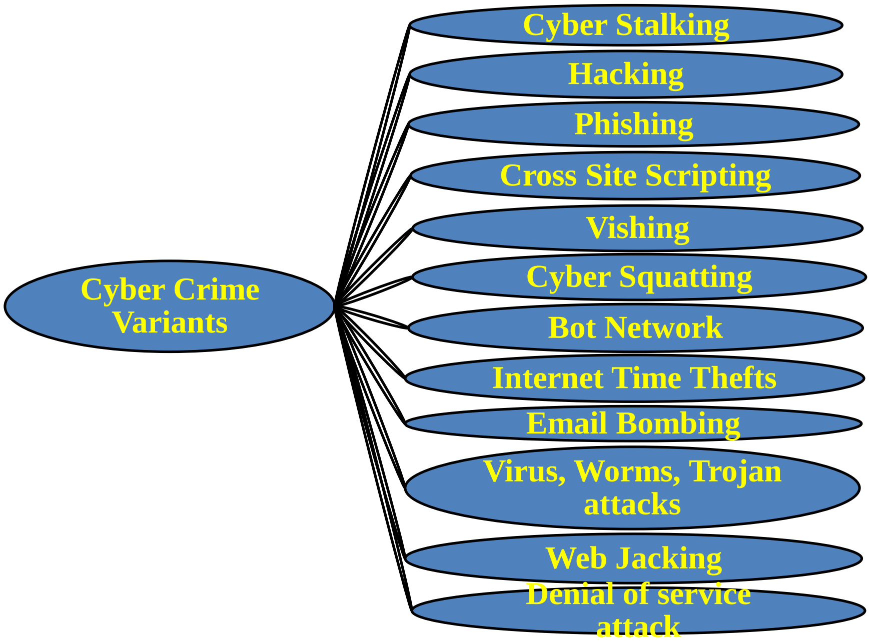


Fig 3: Cyber Crime Variants

5. Role playing factors and growth of cyber crime

The integrity, authenticity, confidentiality and availability of data in cyberspace have become vital questions of the 21st century. The trends of Information Systems such as Internet and cloud computing has created challenges in maintaining security of information. Data interception, data modification, data theft, network crime, access crime etc are the fundamental categories of cyber crimes. **A**ccountable factors which are responsible for cyber crime are-

1. Data access and sharing policies between private and public sectors.
2. Data leakage through mobile and wireless frauds and cloud computing also plays important role to augmentation of cyber crime.
3. Criminals Justice sanctions like internet restrictions and electronic monitoring.
4. Sentencing of cyber criminals etc.

Threats from cybercrime are increasing rapidly and Internet has become a platform for criminals to conduct their activities and to launch attacks with relative obscurity. Main targets of Cyber criminals are citizens, businesses and governments. Social networking and constant online communication, proliferation of communication devices, networks, and users have generated new vulnerabilities that create more cyber crime opportunities. In 2013, the IC3 received 262,813 consumer complaints with an adjusted dollar loss of $781,841,6111, which is a 48.8 percent increase in reported losses since 2012 ($581,441,110). Of the 262,813 complaints received in 2013, 45.5 percent (119,457) reported financial loss. Year wise complaints registered in IC3 has been shown below [7]-

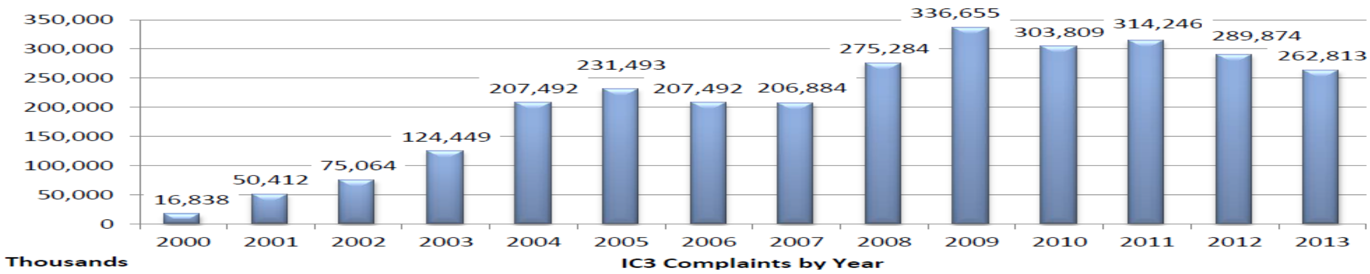
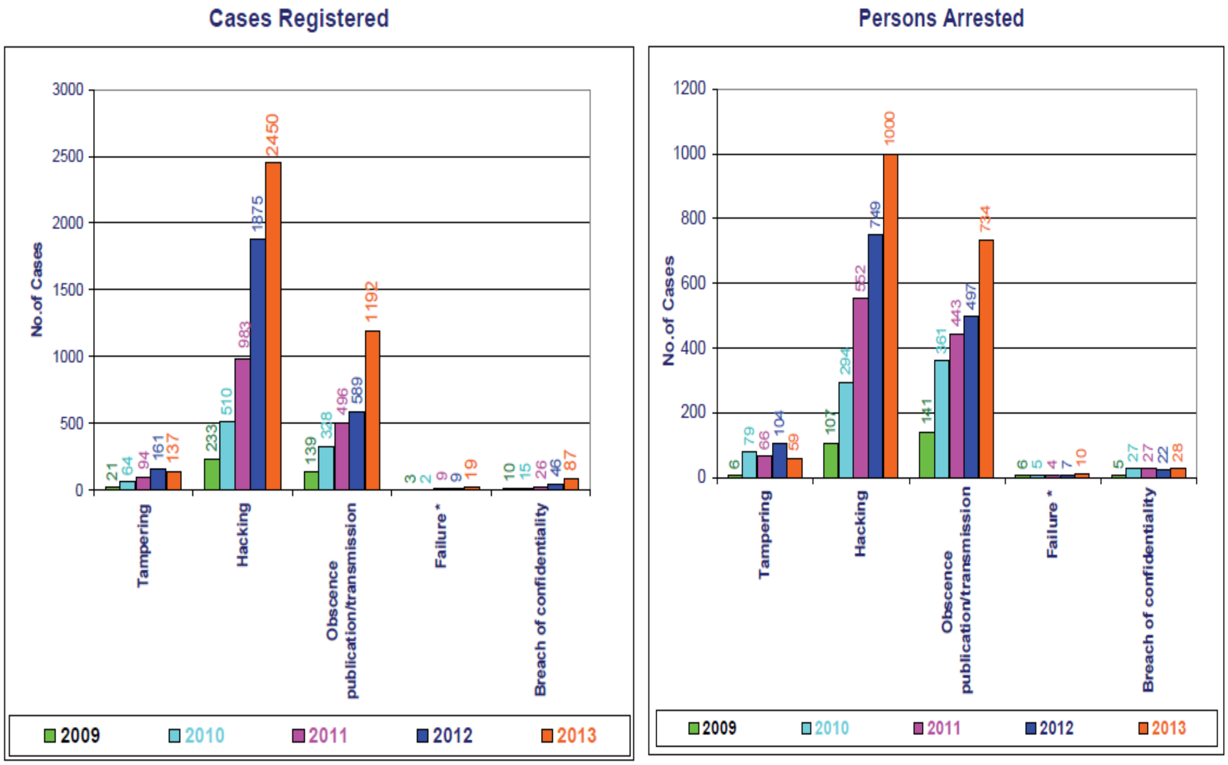


Fig 4: Year wise Status of IC3 complaints against cyber crime

According to Computer Emergency Response Team-India (CERT-In) report till may 2014 total 9,9,174 Indian websites were hacked by hacker groups spread across the world[5]. The study revealed 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[6]. In fig 5 Cyber crimes / cases registered and persons arrested under IT Act during 2009-2013 have been shown. According to National Cyber Crime Bureau Report (2013) from 2009 to 2013 the graph for registered cases under IT Act has been increased successively and most of the cases were for hacking and obscene publication/transmission. Like in 2013 total 2450 cases were registered and only 1000 persons were arrested under hacking similarly 1192 cases were registered under obscene publication/transmission and only 734 persons were arrested [8].



* Failure includes the data (i) Of Compliance/Orders of certifying Authority (ii) To assist in decrypting the information by Govt. Agency

Fig 5: Cyber crimes / cases registered and persons arrested under IT Act during 2009-2013

In fig 6 Cyber crimes / cases registered and persons arrested under IPC during 2009-2013 have been shown. According to National Cyber Crime Bureau Report (2013) from 2009 to 2013 the graph for registered cases under IT Act has been increased successively and most of the cases were for forgery (735 cases) and of criminal breach of trust/fraud (518 cases). As it is clear that out of 735 registered cases only 608 persons were arrested under forgery and out of 518 registered cases only 471 persons were arrested under criminal breach of trust/fraud [8].

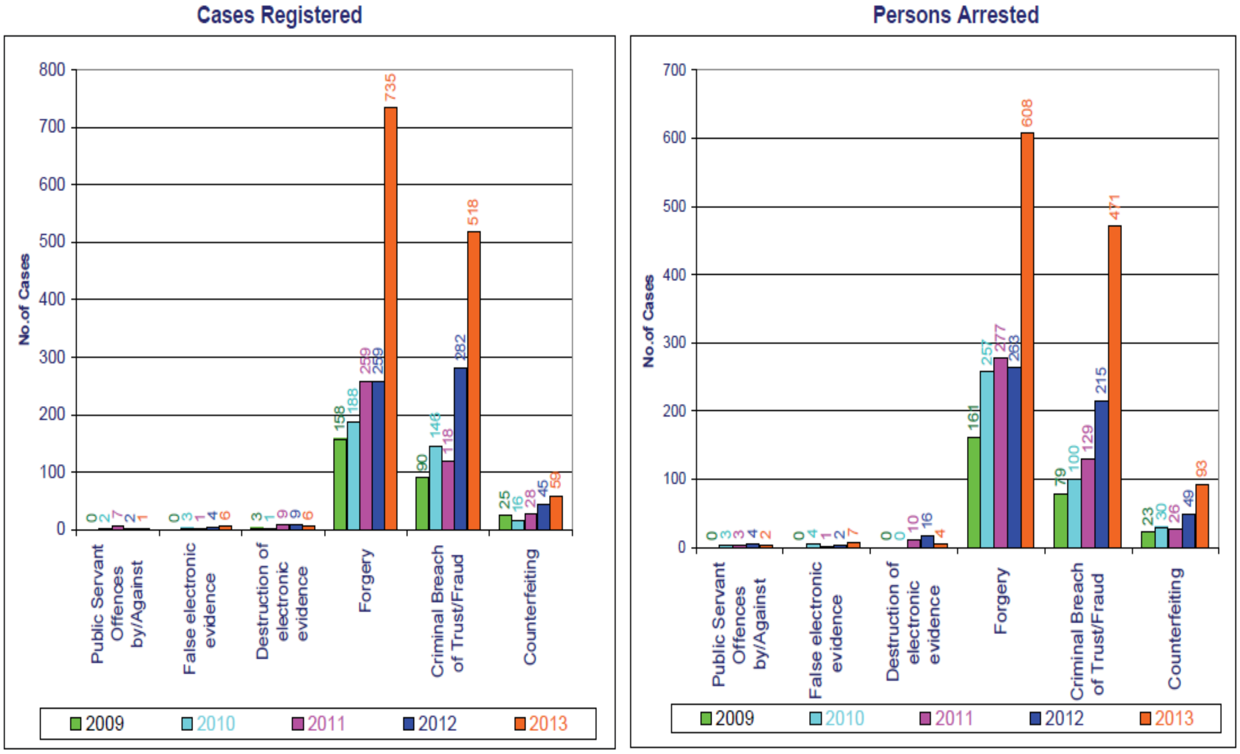


Fig 6: Cyber crimes / cases registered and persons arrested under IPC during 2009 - 2013

From fig 5 and fig 6, It can be observed that the ratio of persons arrested under IPC is more than the number of persons arrested under IT act that indicates that special attention is required under IT act.

6. Challenges and Issues

Development of national technological and manpower capabilities, endorsement of new laws, encouragement of higher level of industry government collaboration programs and move forward for international cooperation are critical to combat cyber crime. Some of the issues are [2]:

A) Technical Issues: The growth of Cyber crime as given rise to numerous forensic software vendors and the main challenge is to select one of them because no single forensic tool is capable to solve the entire case. Technical issues are related with hardware, software and third party tools, where large storage space is required to store analysed image and retrieved evidence because retrieved evidence might contain documents, pictures, videos and audio files which require large storage space.

B) Global Issues: Correspondence with bodies such as Google, Yahoo, Hotmail is quite time consuming and prolong the investigations. Most of the IP addresses retrieved during investigation leads to servers or computers located abroad which have no identity, hence further investigations are blocked and closed.

C) Challenges Faced By Law Enforcement: In some cases people are unaware of the resources and services that law enforcement could provide them if being a victim of crime or witness and fear to report crimes.

D) Wireless or Wi-Fi, Bluetooth, Infrared Issues: This is another cause for vulnerability and exploitation that law enforcement faces due to latest unsecured wireless technologies

E) Inadequate Training and Funds: Training bodies are limited and are expensive. Insufficient funding is also responsible factor for officers training and future investment point of view. Transfers and recruiting officers adds to the loss of experienced staff and spending for training the newcomers. Cases become pending in such circumstances.

F) Judiciary and IT Act 2000: The judicial bodies are not fully aware of Cyber crime and the way in which investigations are carried out. Although Cyber law courses available in India, it is difficult to find an experienced cyber lawyer who is aware of Forensic analysis and technical terms. It is difficult to convince judicial bodies including judges and the tribunal when evidence is in a digital format. There is no legal procedure for collecting, analyzing and presenting evidence in the court of law. There are certain shortcomings of the Information Technology Act, 2000 with regard to identity theft, spamming, pornography, data protection and internet banking.

7. Detection and Prevention of cybercrime

The increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. The attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, the study revealed [6]. Fig 7 shows four major tasks perform by cyber analysts for working with digital evidence.

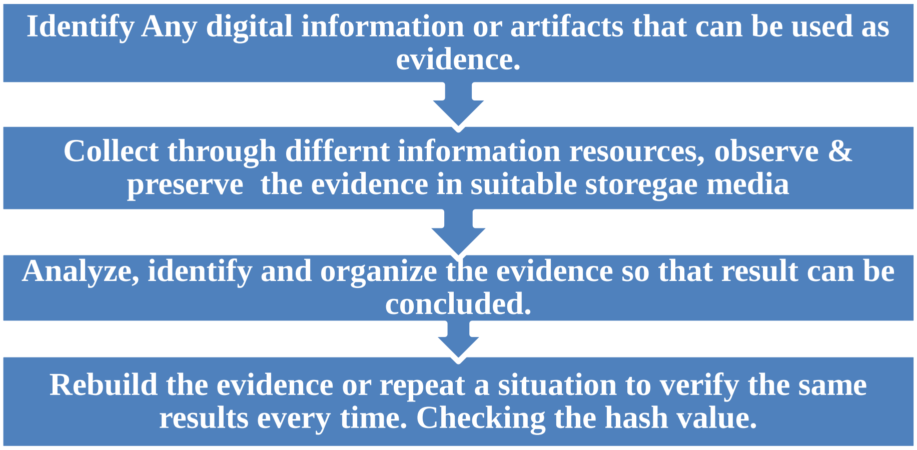

Identify Any digital information or artifacts that can be used as evidence.
Collect through differnt information resources, observe & preserve the evidence in suitable storegae media
Analyze, identify and organize the evidence so that result can be concluded.
Rebuild the evidence or repeat a situation to verify the same results every time. Checking the hash value.

Fig 7: Major Tasks Perform By Cyber Analysts For Working With Digital Evidence

Prevention mechanism should at least consider security mechanisms like identity proof verification, Safe confidentiality of transferred data, Integrity of transferred data, Undeniable responsibility for transactions made. Some of the important cyber crime safety mechanism used by most of the International and international banks are password encryption, virtual keyboard, secure socket layer, SMS alerts, user awareness programs, browser protection, OTP token, OTP card , digital certification etc.

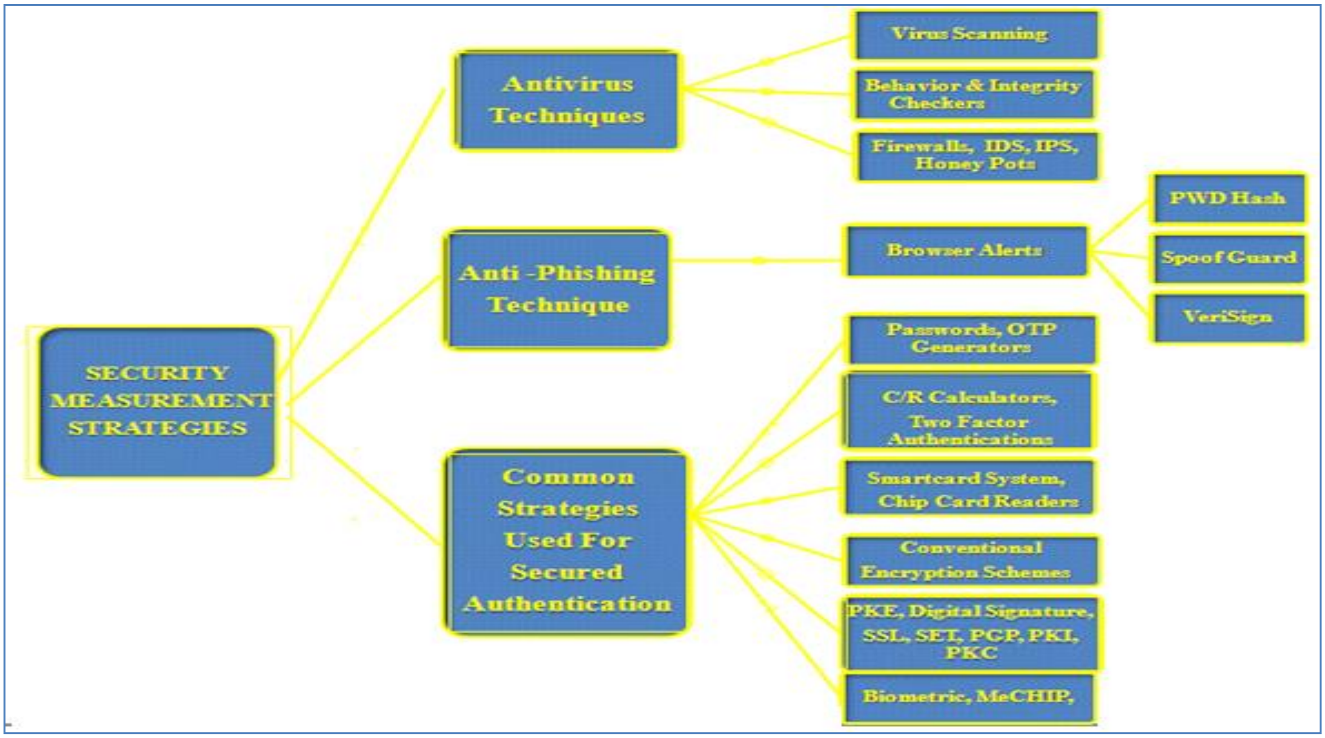

SECURITY MEASUREMENT STRATEGIES
Antivirus Techniques
Virus Scanning
Behavior & Integrity Checkers
Firewalls, IDS, IPS, Honey Pots
Anti -Phishing Technique
Browser Alerts
PWD Hash
Spoof Guard
VeriSign
Common Strategies Used For Secured Authentication
Passwords, OTP Generators
C/R Calculators, Two Factor Authentications
Smartcard System, Chip Card Readers
Conventional Encryption Schemes
PKE, Digital Signature, SSL, SET, PGP, PKI, PKC
Biometric, MeCHIP,

Fig 8 - Security Measurement Strategies

The most popular weapon in cyber terrorism is the use of computer viruses and worms. Antivirus stays helpless until and unless its database is updated periodically to discover new attacks like hijacking, Denial of Service etc. therefore other software's are also needed along with the use of antivirus. It is good practice not to eliminate the firewall from our system even if it has limited capacities compared to IPS or IDS, because a firewall reduces the amount of the bad traffic that can reach the IPS and IDS, which will reduce the alarms and the suspicious data. Some of the foremost policies involved in cyber safety mechanism are NCSP (National Cyber Security Policy)-2013, IT Act 2000 and ITA Act 2008, Counter Measures used to provide cyber safety mechanism, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), An intrusion detection and prevention system (IDPS), Distributed Intrusion Detection System (DIDS) and GPRS Security Architecture etc[9][10][11].

The economic growth of any nation and its security depends on how well is its cyberspace secured and protected. In recent cyber security measures Non Government (private) regulatory measures, National Law and enforcement measure, Defensive strategies, products as well as some limited forms of international cooperation and regulations plays important role. Some of the initiatives taken by Non Government Organization are IETF (Internet Engineering Task Force), Web Consortium House, FIRST (Forum of Incident Response and Security Teams), IEEE (Institute of Electrical and Electronics Engineers), ICANN (Internet Corporation for

Assigned Names and Numbers). Government Organizations are DSCI (Data Security Council of India), NIC (National Informatics Centre), Cert-In (Indian Computer Emergency Response Team), NISAP (National Information Security Assurance Program). International Organizations are IUSCSF (Indo-US Cyber Security Forum) and USNSE (United State National Security Experts) [9][12].

8. Recommendations

A combination of technological and non-technological measures can give strong fight to the problems arising through cyber crime. Few recommendations are:

1. The new legislation to cover all the aspects of the Cyber Crimes should be passed to remove the grey areas of the law.
2. There is also a need for IT-savvy lawyers and judges, as well as training for government agencies and professionals in computer forensics.
3. From technological point of view database and network design with their implementation part is crucial, whereas nontechnical measures are behavioral measures like general awareness training programs for employees, consumers and public.
4. The software's which are easily available for download should be restricted by the Government by appropriate actions.
5. Smartphone users are advised to check for security certificates while downloading apps (games, music and other software) from third party or unsecured sites
6. New amendment should be including in to the IT Act to make it efficient and active against a Cyber Crime.
7. Investing in training people, law enforcement authorities and investigators could also enhance nations’ ability to fight with cybercrimes.
8. There is an immense need for training, and more cities need to have such cells hence the training camps and public awareness programs should be organized in the Companies as well as in common sectors.
9. Multi-layered boundary defense control should be established to control the flow of traffic.
10. Standardized logs for each hardware and software should be generated to maintenance, monitoring, and analyze security including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction.

9. Conclusion

Cyber crime is emerging as a serious threat. Awareness is important, and any matter should be reported at once. More importantly, users must try and save any electronic information trail on their computers. Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defenses and are rapidly becoming obsolete because, cyber criminals now use encryption technology to avoid detection. There is a dire need for evolving a code of Ethics on the Cyber-Space and discipline and it is necessary to take certain precautions while operating it. Since cyber world has no boundaries, it is a Herculean task to frame laws which can cover each and every aspect. But, however a balance has to be maintained and laws be evolved so as to keep a check on cyber crimes. World Wide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. Unless there is solid prevention, cyber crime will rise steeply. A strong commitment is required from beside of general public, Bench and Bar, IT experts, Executive Members, Social Organization, NGOs, and other similar type of organization to keep the society free from such type of crime.

10. References

1. McAfee Intel Security (June 2014) "Net losses Estimating the global cost of cyber crime: Economic Impact of cyber crime II, centre for strategic and international studies", pp 24, http://www.mcafee.com, http://csis.org/.
2. Raksha Chouhan, Shashikant Pardeshi (2013) "Cyber Crime Security and Upcoming Challenges: An Overview", Journal of Engineering, Science And Management Education (JESME), Quarterly Research Journal of NITTTR Bhopal, Vol-6, Issue-III, July–September 2013, PP 131-136, ISSN 0976-0121.
3. Raksha Chouhan (2014) "Cyber Crimes: Evolution, Detection and Future Challenges", The IUP Journal of Information Technology, ICFAI University Press, Hyderabad, Andhra Pradesh, Vol. X, No. 1, March 2014, PP 48-55, ISSN 0973-2896.
4. Criminal Defense (visited: 8-1-15) "The evolution of cybercrime from past to the present" http://www.criminallawyergroup.com/criminal-defense/the-evolution-of-cybercrime-from-past-to-the-present.php.
5. Computer Emergency Response Team-India (CERT-In) reports 62,189 cyber attacks till May 2014, http://www.techmistory.com/2014/07/cert-in-reports-62189-cyber-attacks.html, visited: 10-1-15.
6. The Economic Times (Jan 5, 2015) "Cyber crimes in India likely to double to 3 lakh in 2015:Report",http://articles.economictimes.indiatimes.com/2015-01-05/news/57705670_1_cyber-crimes-online-banking-pin-and-account-number.
7. FBI IC3 (Federal Bureau of Investigation International Crime Complaint Center 2013) "2013 Internet Crime Report", visited on 10-1-15.
8. National Cyber Crime Bureau Report (2013) "Crime in India-2013", http://ncrb.gov.in/, pp 6, visited: 10-1-15.
9. Atul M. Tonge, Suraj S. Kasture , Surbhi R. Chaudhari(2013), "Cyber security: challenges for society- literature review", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75 www.iosrjournals.org.
10. Janhavi J Deshmukh and Surbhi R Chaudhari (April' 2014), Cyber crime in Indian scenario – a literature snapshot, International Journal of Conceptions on Computing and Information Technology, Vol.2, Issue 2, pp 24-29, ISSN: 2345 – 9808.

11. Baroudi Siba, Ziade Haissam, Mounla Bassem (2004), “Are we really protected against hackers?” Proceddings International Conference on Information and Communication Technologies: from theory to application. PP. 621-622. IEEE

12. Col S S Raghav (visited: 28-11-14), “cyber security in india's counter terrorism strategy”, pp 5, ids.nic.in.