A DETAILED REPORT ON CYBERCRIME AND CYBERSECURITY

Shlok Shivkar
Author
Department of Information Technology,
Vidyalankar Technology School of Information,
Vidyalankar Educational Campus,
Vidyalankar College Rd, Wadala East,
Mumbai, Maharashtra 400037.
Email: shlok.shivkar@vsit.edu.in
Mobile: +91 8369621421

Taha Poonawala
Author,
Department of Information Technology,
Vidyalankar Technology School of Information,
Vidyalankar Educational Campus,
Vidyalankar College Rd, Wadala East,
Mumbai, Maharashtra 400037.
Email: taha.poonawala@vsit.edu.in
Mobile: +91 9819961919

1. ABSTRACT

Cyber Security plays an important role in the field of information technology. Securing the information has become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is ‘cyber crimes’ which are increasing immensely day by day. Governments, military, organizations, financial institutions, universities and other businesses collect, process and store a large amount of confidential information and data on computers and transmit that data over networks to other computers. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on the latest cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: cyber security, cybercrime, cyber ethics, social media, cloud computing, android apps.

2. INTRODUCTION

Cyber security, known as “information technology security”, emphasizes on securing networks, data, programs and computers from unauthorized or unintended variation, loss, change or access. Government agencies, corporations, hospitals, financial institutions, military and other groups store, gather and practice a big deal of intimate information on the computers and send that data over the network to the other computers. With the growing volume and criticality of cyber-attacks, the emphasis is needed to secure confidential information and trade, also securing the security of the nation. Security in Computer Role of Cyber Security in Today’s Scenario Manju Khari NITP, India Gulshan Shrivastava NITP, India Sana Gupta AIACTR, India Rashmi Gupta AIACTR, India also known as “cyber security” either “IT security” which means preservation of information entities from damage or theft of the software, the hardware and to the information cured on them, also from the misdirection or disruption of the duties they offer. It involves the regulation of the physical approach to the hardware, also preserving from attack that can come from accessing network, code injection & data, and because of illegal activities by vendors, whether intentional, accidental, or due to them by guessing the secure methods. The domain is of developing relevance because of the growing dependency on the internet and computer systems in most of the wireless networks, societies like Wi-Fi, Bluetooth and the growth of intelligent devices, involving televisions, small devices and smart phones as an important section of the IoT. While increased technological developments have given many areas for organizations of all sizes, potential sources of efficiency and better opportunity. Cyber security – explained as the “protection of systems, networks and data in cyberspace – is a critical issue for all businesses”. Cyber security will become vital as more devices, become connected to the computer internet, ‘the internet of things’.

3. NATURE OF CYBERSPACE

Privacy and security of the data will always be top security measures that any organization takes care of. We are presently living in a world where all the

information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures

Incidents	Jan- June 2012	Jan- June 2013	%Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)

Total	5581	5592	

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year
- The majority of companies are preparing for when, not if, cyber attacks occur
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on a massive scale. The fact tables share the same operating system as smart phones means they will soon be targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smartphones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

4. NEED OF CYBER SECURITY

Cybersecurity is now considered an important part of individuals and families, as well as organizations, governments, educational institutions and our business. It is essential for families and parents to protect the children and family members from online fraud. In terms of financial security, it is crucial to secure our financial information that can affect our personal financial status. The Internet is very important and beneficial for faculty, students, staff and educational institutions, and has provided lots of learning opportunities with a number of online risks [5].

There is a vital need for internet users to understand how to protect themselves from online fraud and identity theft. Appropriate learning about online behavior and system protection results in reduction in vulnerabilities and safer online environment. Small and medium-sized organizations also experience various security related challenges because of limited resources and appropriate cyber security skills. The rapid expansion of technologies is also creating and making cyber security more challenging as we do not present permanent solutions for concerned problems. Although we are actively fighting and presenting various frameworks or technologies to protect our network and information, all of these provide protection for the short term only. However, better security understanding and appropriate strategies can help us to protect intellectual property and trade secrets and reduce financial and reputation loss. Central, state and local governments hold large amounts of data and confidential records online in digital form that becomes the primary target for a cyber-attack. Most of the time governments face difficulties due to inappropriate infrastructure, lack of awareness and sufficient funding. It is important for the government bodies to provide reliable services to society, maintain healthy citizen- to-government communications and protection of confidential information.

5. CYBER SECURITY

There are three core principles of cyber security. It involves Integrity, Confidentiality and Availability. Integrity means information unaltered from its original state without authorization. Information not to be shared with inappropriate users. Availability refers to systems and information available and accessible to who need it essentially.

5.1) Types of Cyber Security

a. Physical Computer Security

It is the easiest and most basic type of computer security. In this anyone who has physical access to the computer controls it. Hidden files, Passwords and other protections not to save out a determined attacker endlessly. Physical computer security is taken seriously by computer hosting companies. They hire guards, use secure doors, and even put computers on military bases or deserted islands just to keep them safe. But the average person can’t protect their private

files on office computers and other places. Either the computer repair technician is not aware about the important files. But the average person pays very little attention to physical computer security. For example, they put private files on their office computers—computers they leave unattended for 16 hours every weekday. Or they hand their computer with illegal files over to a computer repair technician without thinking that anyone who can fix a computer can access all of their files. The same applies for External Hard Drives Security. It is ignored completely but people continue to store precious files on these devices and then proceed to leave them lying around for anyone to grab.

b. Network Security

It is a branch of computer security specifically related to the Internet. The goal of network security is to measure and establish rules to protect against attacks over the Internet and internet accessible resources. It is controlled by the network administrator. It is useful for both private and public. It includes wired and wireless networks of Network Protocols, IP security, Email security, Web security, Intruders, Viruses and Firewalls. A firewall is a critical part of computer security. The main functionality of firewall is blocking unapproved network access attempts from computers. Home computers can be easily protected by firewalls. The easy method of protecting a network resource is using a unique name and password. To secure and manage the computer over the network, restrict access to servers and routers. when accessing any critical system requires strong authentication and to access the network use SSH to tunnel through firewalls.

c. Executable Security

Executable security is always known as anti-virus security. Virus blocking is important. Antivirus software is developed by a group of programmers because of its complexity. Microsoft's progress has significantly increased executable computer security in the last decade The new features are added in new versions of programs it includes anti executable policy modification error has resolved, resolved an issue when initiating a Local Control List Scan where executables from the mounted Storage Space were not added to control list. It will continue to make our computers more reliable in the years to come.

5.2) Cyber security standards

When identifying the most useful best-practice standards and guidance for implementing effective cyber security, it is important to establish the role that each fulfills its scope and how it interacts with other standards and guidance. Cybersecurity standards are generally applicable to all organizations regardless of their size or the industry and sector in which they operate. This page provides generic information on each of the standards that is usually recognized as an essential component of any cyber security strategy. Security standards can be used as guidelines or framework to develop and maintain an adequate information security management system (ISMS). The standards ISO/IEC 27000, 27001 and 27002 are international standards that are receiving growing recognition and adoption. They are referred to as “common language of organizations around the world” for information security.

6. CYBER THREATS

Cyber threats mean the possibility of a malicious attempt to disrupt or damage a system or a computer network. The goal of attacks is depending on the requirements of cyber criminals. The attacks affected many important areas like military, financial institutions, governments, corporations, business and hospitals to collect, store and process sensitive information of computers and sharing the data to other computers through networks.

6.1) Types of Cyber Threats and Techniques

Information and Data security is of high concern for almost all organizations. The attackers are creating a new technique to detect the patterns, signature and information in the cyberspace. Here we are explaining some of the threats and techniques for cyber land.

a. Trojan Horses – Trojan Horses are harmful codes or a malicious program are hidden behind genuine programs which can cause damage to the system or allow complete access to the system for data corruption and stolen the data, log your keystrokes and watch through webcam. It is not easily detectable and acts as a backdoor

b. Rootkits – A rootkit is a malicious software developed to hides certain programs or a process to a privilege to access a system and from regular anti-virus scan detection. Whenever booting a system that software which runs and gets activated each time and is difficult to install and detect various processes and files in the system.

c. Spyware – Spyware refers to a hidden component of a freeware program which naturally gather and spy information from the system without the knowledge of users through an internet connection. Such spyware inundated with uncontrollable pop-up ads.

d. Scareware – Scareware is a type of threat which acts as an honest system message and guides to purchase and download potentially dangerous and useless. But actually they are harmful and take control of all the software's running on certain computers.

e. Spoofing – It is a cyber-attack where a program or a person impersonate another by creating false data in order to gain illegal access to a system. This type of threats is generally found in emails where the sender's address is spoofed

f. Tampering – Tampering is an attack of web based where without the customer's knowledge certain parameters in the URL are changed and when the keys in that URL of customer it appears exactly the same. It is basically done by criminals and hackers to steal the identity and gain illegal access to information.

g. Repudiation Attack – This attack occurs when the user denies the fact that the user has initiated a transaction. A user basically has the knowledge of communication or transaction to deny for later claim communication or transaction have not ever taken place.

h. Backdoors – In this threat the attacker can install keylogging software by using a back door to allow a system for illegal access. This threat is potentially serious as it allows for files modification, information stealing, unwanted software installing or sometimes taking control of the entire computer.

i. Denial-of-Service Attack – A DOS attack or a denial-of-service attack commonly means attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the internet. The types of attack include Ping of Death, Smurf, Buffer overflow, Teardrop, SYN attack, and many more. To avoid DOS attacks installing security patches, Intrusion detection system and Firewalls.

j. Eavesdropping –Eavesdropping refers to the unauthorized real-time interception of a private communication between the network and a host. Security measures in contradiction of internet communications are use encrypted connection during data transmission, update antivirus software with a malicious code definition, Install intrusion prevention system and use authentication services.

k. Privilege Escalation Attack – A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. It is not compulsory that all the system hack will provide full access to the targeted system of unauthorized users. There are five ways to escalate privileges:

1. Dumping the SAM file

2. Retrieving the /etc/passwd file

3. Week Permission on processes.

4. Sensitive Information stored in shared folders.

5. DLL Preloading.

To protect against privilege escalations are Anti Forgery Token, Encryption of Query string parameters, HTTP referrer check, URL activity Tampering, HTML Encoding and many more.

l. Exploits – Exploit is essentially a chunk of data or a piece of software specifically to take advantage of a certain vulnerability due to that the system

offers to intruders. It is categorized according to the types of vulnerability, whether to run on a remote system or the same system which one has the vulnerability and the result of running the exploit.

m. Malware – Malware is a malicious software that is designed to do unwanted actions into the system or to damage the system. Malware is of many types like Trojans, viruses, etc., which can cause havoc on a computer's hard drive. They can either Steal sensitive information, alter or delete some directory or files, send emails on your behalf and Take control of your computer and all the software running on it.

n. Adware – Adware is a software that will collect all your data without our consent. That would come in the form of installed automatically or a free download and send your passwords, usernames, surfing habits, settings, downloaded applications to third parties. Take you to unwanted sites or inundate you with uncontrollable pop-up ads. These are difficult to remove and can infect your computer with viruses.

o. Botnets – Bots is an application software that runs automated tasks which are repetitive and not complicated. The infected system is remotely controlled by the creator. Bots to spread malware, send emails with attached viruses and it can support DOS attacks against other systems.

p. Ransomware – Ransomware is a type of malware which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. It's affected by phishing emails or web-site pop-up advertisements. There are two types of ransomware.

+ Lock Screen Ransomware: Displays an image that prevents you from gaining access to your computer.

+ Encryption Ransomware: Encrypts files on your system's hard drive and sometimes on shared network drives. To prevent from opening the files USB drives, external hard drives and even some cloud storage drives to keep an up-to-date backup.

7. CYBER SECURITY TECHNIQUES

7.1 Access control and password security

The concept of user name and password has been a fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

7.2 Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus a good anti-virus software is also essential to protect the devices from viruses.

7.3 Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

7.4 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

7.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the

program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti-virus software is a must and basic necessity for every system.

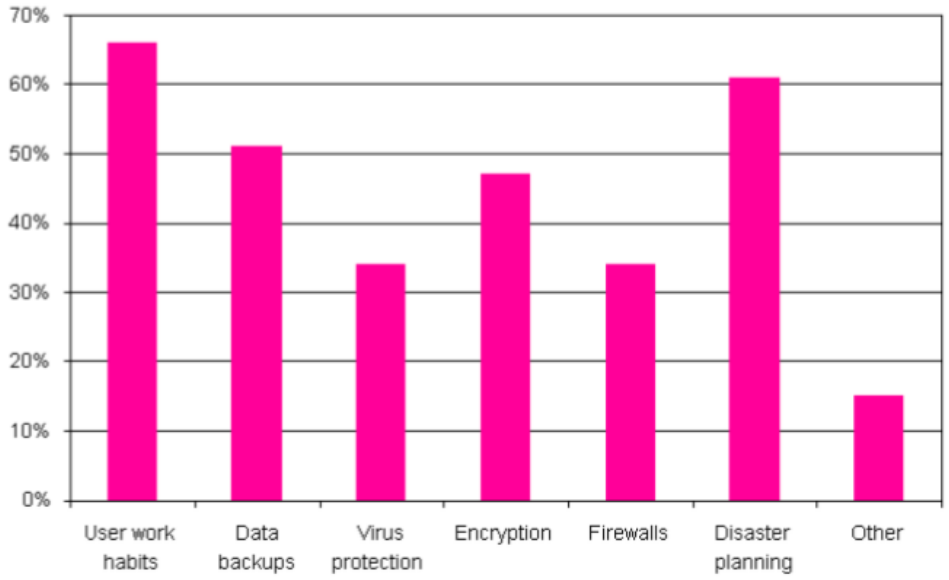

Fig 1: Techniques on cyber security

8. Growth in Cyber Crime

A large number of tasks now have been automated and now easier to handle with the help of information technology. Now, hardly any sector of society remains unaffected. By the end of 2013, over 2.7 billion people are using internet worldwide while 4.4 billion still needs to be connected. Now a day, our lives look incomplete without internet, mobiles and computers. Records are maintained digitally and transferred on communication lines. Banks and other financial institutions also use internet and connected network to carry out financial transactions. So it becomes necessary to secure our network from treats and hacking. According to report about 1,00,000 virus/ worms are reported to be active each day and out of which 10,000 are identified as new and unique. The report also describes the number of websites hacked (Fig. 2 and Fig. 3) in last six years across worldwide and in India as well.

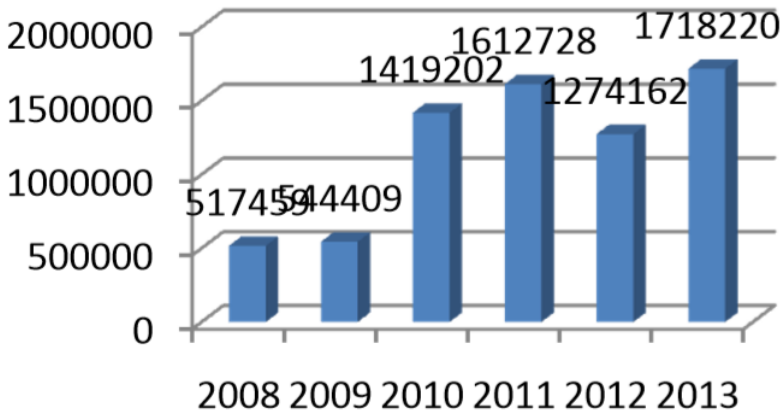

Fig 2: Websites hacking worldwide

ISTR highlight 2013 as the year of Mega Breach. In this year total number of breaches was about 62 percent which was larger than in 2012 with 254 breaches. It was also greater than in 2011 with 207 breaches [15]. Although, 2013 was the year in which eight breaches exposed greater than 10 million identities but in 2012 only one breach was capable to expose about the same number of identities. In 2013, about 552 million identities were breached that has transferred financial and credit card information, date of birth, contact number and IDs into criminal hands. Normally, cyber attackers seek vulnerability in legitimate websites to have control to plant malicious software.

Note: the data of Fig.2 and Fig.3 has been taken from Fifty Second Report. Cyber Crime, Cyber Security and Right to Privacy, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Govt. of India, February 2014.

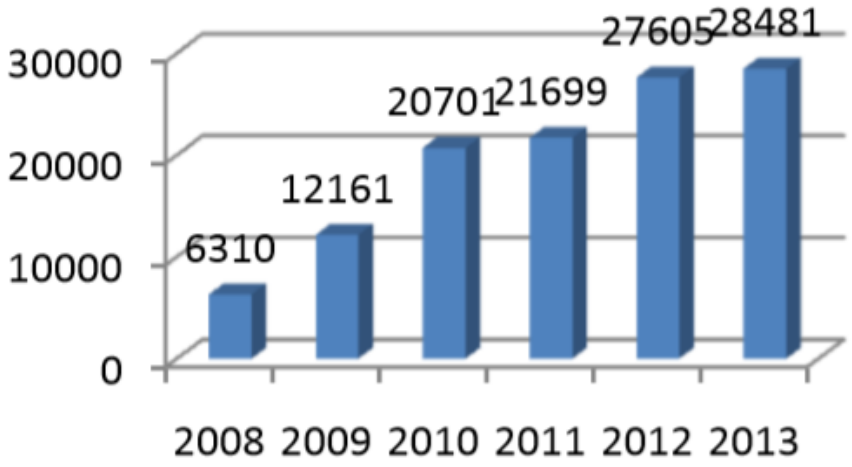

Fig 3: Websites hacking in India

ISTR vulnerability assessment system found that about 82 percent websites have vulnerabilities that invite the terrorists for coordinated attack. In 2012, Malware was detected on 1 in 532 websites while it was found in 566 websites in 2013.

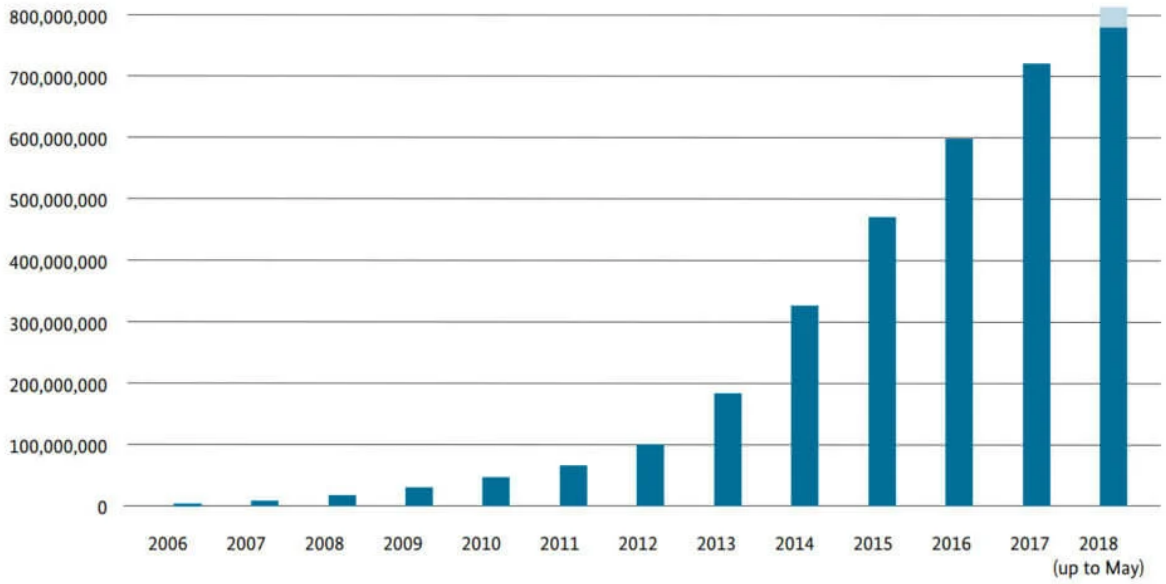

Fig 4: latest data on websites hacking world wide

9. Cybercrimes in India

In 2013, total 4,356 cases were reported under IT Act while this figure was 2,876 in 2012. In other words, there was rapid growth of about 51.5% from 2012 to 2013. Of the 681 cases, about 15.6% were registered from Maharashtra. In Andhra Pradesh 635 cases were registered under the same Act, followed by Karnataka 513 cases and Uttar Pradesh with 372 cases. About 45.1% (1,966 cases) were related to hacking of websites and damage of computer resources [16]. There were 1,337 cases related to cybercrime, registered under different sections of IPC during 2013 while this figure was around 601 in 2012. This shows a rapid increase, around 122.5% in a year [16]. Only in Uttar Pradesh 310 cases were registered from 1,337 cases. Maharashtra holds second position with 226 cases followed by Haryana with 211 cases. Most of the cases, out of total 1,337 cases, were related to forgery and financial fraud. From the 1,337 cases, 747 cases were registered under the forgery category while 518 cases fell in fraud.

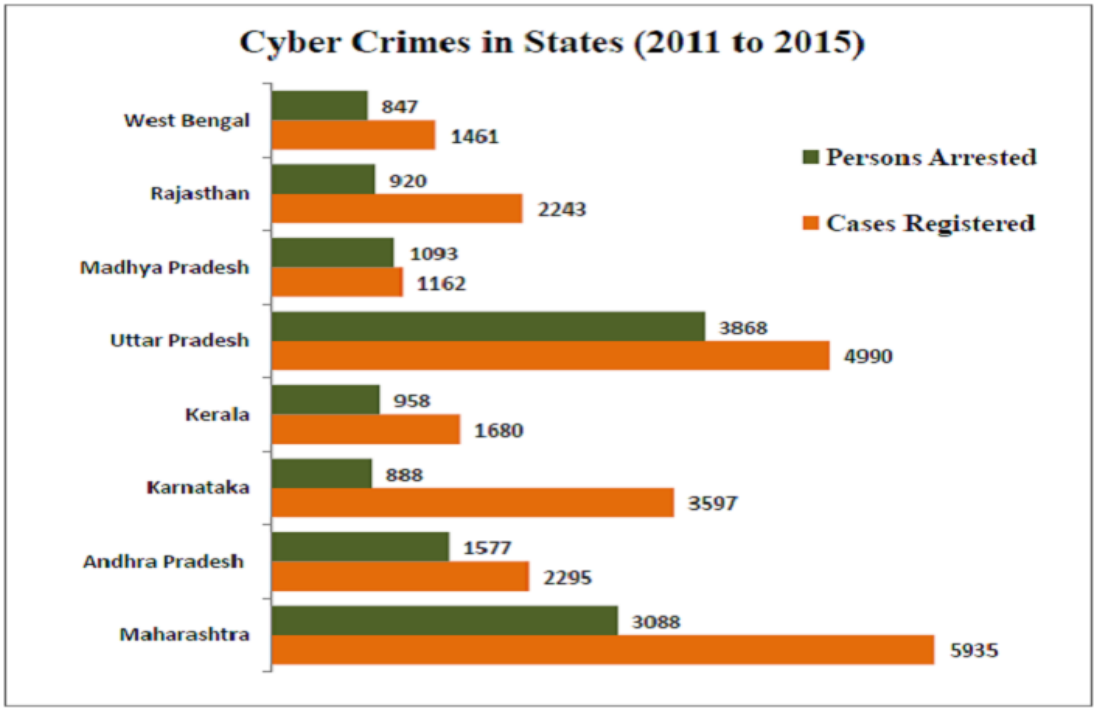

Fig 5: Cyber Crime Growth in India

Although, all these offenses were put in traditional IPC crimes but somewhere these were related to cybercrime wherein computer systems and internet were used to conduct such offenses. Maharashtra was the state with the highest number of cyber forgery followed by Uttar Pradesh with. Statistics depicted in fig 4. Show that cybercrimes are rapidly growing in numbers and sophistication as well. We still require a technique or procedure to control cybercrimes. As the statistics of the arrested people show that there is a huge gap between cases registered and the person arrested. It means we are not reaching and arresting all the criminals who commit such types of cybercrimes.

10. CONCLUSION

In this paper, we have detailed about the nature of cyberspace and defined the cyber security with its necessities across the world. Significant statistics show that India stands on third position in the usage of internet and also experiencing the problem of cyber security. We have also explained various methods of cyber-attacks and showed how the websites hacking incidents are common and growing with time worldwide.

References

[1] Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, Pittsburgh, November 2002.

[2] A Report from United Nations offices on drugs and crime (UNODC), the use of the Internet for terrorist purposes, New York, USA, 2012.

[3] Report available on http://searchsoa.techtarget.com/definition/cyberspace.

[4] A Report available on http://www.businessdictionary.com/definition/cyberspace.html.

[5] A Report form CISCO, Cybersecurity: Everyone's Responsibility, 2010.

[6] A Fifty Second Report. Cyber Crime, Cyber Security and Right to Privacy, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Govt. of India, February 2014.

[7] A Report, Digital India 2014, IAMAI 2013.

[8] Gisela Wurm, Stalking, A Report before Committee on Equality and Non-Discrimination, June 2013.

[9] A Report available at http://searchsecurity.techtarget.com/definition/mail-bomb.

[10] A Report available at http://www.businessdictionary.com/definition/e-mail-bomb.html

[11] A Report available at http://www.sse.gov.on.ca/mcs/en/pages/identity_theft.as px

[12] Report available at https://www.researchgate.net/publication/322466321_CYBER_SECURITY_AND_THREATS

[13] Report available at https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[14] Report available at https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.9225&rep=rep1&type=pdf

[15] A Report available at http://www.rcmp-grc.gc.ca/scams- fraudes/id-theft-vol-eng.htm.

[16] A Report available at http://www.webopedia.com/DidYouKnow/Internet/virus. asp.

[17] A Fifty Second Report. Cyber Crime, Cyber Security and Right to Privacy, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Govt. of India, February 2014.

[18] A Report on Internet Security Threat Report 2014, Symantec Corporation, Volume 19, April 2014.

[19] A Report on, Crime in India 2013 compendium, National Crime records Bureau, Ministry of Home affairs, Govt. of India.