International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Review of Indian Approach towards Cybersecurity

Onkar Singh†, Priya Gupta‡* and Roushan Kumar†

†Department of Computer Science, Shaheed Sukhdev College of Business Studies, University of Delhi, India
‡Department of Computer Science, Maharaja Agrasen College, University of Delhi, India
†NCWEB, University of Delhi, Mewar University, India

Accepted 20 April 2016, Available online 24 April 2016, **Vol.6, No.2 (April 2016)**

Abstract

Security, safety and privacy are of paramount importance to anyone who likes to crawl on the web. Keeping the best interest of the internet users in mind, India has laid down very solid foundations to safeguard its people from cyberattacks and cyber terrorism. Many cyber laws like National Cybersecurity Policy and Information Technology Act have been very effective in keeping unwanted invaders at bay. Even though India has solid policies against cybercrimes, the main challenge it faces is that general awareness is non-existent. Moreover, the policies laid down take too much time to implement rules and regulations for the betterment of the people. This research paper recommends some excellent point's like- Proper blend in between the Western and Eastern technology, as well as efficient utilization of the resource pool to enable India fight against cyberattacks better. .

Keywords: *Cybersecurity, Cybercrime, Cyberattack, Cyber law, Privacy, Security, Hacking, Computer, Internet*

1. Introduction

India with a population of 1.25 billion, have 0.35 billion (which means 28% of total population) internet users. This is 10.83% of total internet users of the world and has global rank 2 in the list of internet users in the world. We have computers and internet in governments (e-governance, online portals, etc.), banking (ATM, Debit Card, Online Banking, Mobile Banking, etc.), education (online lectures, smart boards, etc.), Entertainment (Facebook, twitters, online cinema ticket booking, etc.), Reservations of tickets (online air ticket, online railway ticket, etc.), Information Retrieval (Google, Wikipedia, etc.), most important of them is Online Shopping. Almost everything has changed & is changing. People in India are using internet for majority of things, but at the same time they are also unaware about the vulnerabilities and risks involved. In this scenario, there is a huge need of some weapons to protect the internet users. To further understand the concept, we should know the following basic terms:

Cybercrime can be defined as any crime which involves computer or internet or both.

Cybercriminal is the person who does cybercrime.

Cyberattack is an attempt by any hacker to damage/destroy IT products and services i.e. computers and computer network.

Cyberspace is our Information and Communication Technology (ICT) infrastructure (as per the report of Cyber Law and Information Technology by Talwant Singh, 2015), which include IT products and services.

Cybersecurity (or Computer Security or Internet Security) is the protection of internet users or computers or computer networks against cyberattack.

Hacker or attacker or intruder is someone who wants to gain unauthorized access of computer or computer network. Hacker can be good (Ethical Hacker) or bad.

Cyber law is the area of law which deals with the use of computers and internet.

At the pace from which internet users in India is increasing, with almost double of that pace cybercrimes are reported. In India, only 50 victims out of 500 on an average registered their complaints. We can now imagine the actual number of cybercrimes in India (http://cyberlawsindia.net/).

Year	No. of cybercrimes reported
2010	966
2011	1791
2012	2876
2013	4356
2014	9622

*Corresponding author **Priya Gupta**; **Onkar Singh** are working as Assistant Professors; **Roushan Kumar** is a Research Scholar (Ph.D-Computer Science)

2. Categorization of Cybercrime

Cybercrimes can be categorized into following two categories:

- Computer as a target
- Computer as a weapon

Computer as target

Physical attack is to damage the computer system. (Section 43-fine up to Rs. 1 crore)

Hacking is an activity of gaining unauthorized access of information into a computer or network. (Section 66-Imprisonment of up to 3 years or fine of up to Rs. 5 lakhs or both)

Virus is a program that makes copies of itself and attached to other programs or files in order to cripple computer or network. It does not come alone in computer rather via some program or file. (Possibly Section 43-fine up to Rs. 1 crore)

Worm is also a program that replicates itself like virus in order to spread itself to different computers via a computer network. It does not attach itself to any program or file. (Possibly Section 43-fine upto Rs. 1 crore)

Trojan Horse or Trojan is any program that misrepresents itself as useful in order to get it install. (Section 43-fine upto Rs. 1 crore)

Denial of Service (DoS) attack can be defined as a situation in which an authorized user is not able to access the resource. For example, send too many requests to a computer resource than it can handle, so that it will get crash or unresponsive.

Computer as a weapon

Pedophilia is a psychiatric disorder in which an adult person has a sexual attraction against prepubescent children generally at an age near to 11.

E-mail Spoofing is sending an e-mail to someone with a fake e-mail id. This fake e-mail looks like original, since list of e-mail in inbox shows only name not e-mail ids.

Defamation is publishing or posting a wrong defamatory content about someone on websites or social websites. (Section 67-Imprisonment of up to 5 years or fine of up to Rs. 10 lakhs or both)

Identity Theft is a cybercrime in which a hacker anyhow steals the username or password of a person. For example, bank details, credit/debit card details, or other sensitive information. (Section 66C-Imprisonment of up to 3 years or fine of up to Rs. 1 lakhs or both)

Theft of internet hours is to use the internet without telling/asking to owner/subscriber.

Data diddling is changing the input data prior to entering or during input. (Section 66-imprisonment of up to 3 years or fine of up to Rs. 5 lakhs or both)

Cyberstalking is the repeated use of electronic communications to harass (prezi.com) or frighten someone, for example by sending threatening emails. (Section 509 of IPC, IT is Act not sufficient)

Cyberterrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear (as per the definition given in oxford dictionary). (Section 66F-Life term imprisonment)

Child Pornography is a type of cybercrime wherein criminals solicit minors [15] via chat rooms for the purpose of child pornography. (Section 67B-Imprisonment of up to 7 years or fine of up to Rs. 10 lakhs or both)

Forgery can be defined as copying or imitating documents or currency using computers, printers, or scanners. (Imprisonment of up to 3 years or fine of up to Rs. 2 lakhs or both)

E-Commerce/Investment fraud is to sale the product online with false/fraudulent offers or gives false/fraudulent online offers to make an investment.

Breach of privacy and confidentiality

Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences (KPMG cybercrime survey report 2015), financial status etc. (Section 72-Imprisonment of up to 2 years or fine of upto ₹ 1 lakhs or both)

Confidentiality: As per Cyber security in India's counter terrorism strategy by Raghav Unauthorized use or disclosure of confidential information like some critical details of business, etc. (Section 72-Imprisonment of up to 2 years or fine of upto Rs. 1 lakhs or both)

Special techniques such as Social Engineering are commonly used to obtain confidential (Cyber security in India's counter terrorism strategy by Raghav) information. **Social Engineering** is defined as to make fool of people so that they will give up private and confidential information for e.g. receive email of winning prize, Phishing, etc.

3. Cyber laws of India

Cybercrime survey report 2015 of KPMG reveals that 72% of Indian business has faced cybercrimes in the last year and 83% respondents of survey stated that there is an external involvement in cyberattacks. In the same report, 94% businesses in India feel this as one of the major threats. In a survey conducted by KPMG, 65% respondent stated that cybercriminals do cybercrimes for financial gain, where as 46% do for corporate espionage. When professionals with knowledge of cybercrimes and cyberattacks are not safe, we can easily visualize how safe a normal internet user is?

Information Technology Act 2000

On June 9, 2000, the Information Technology Act 2000 (or also known as ITA-2000, or IT Act) is passed by the Government of India. This act was the first act of India to deal with cybercrime and electronic commerce. The base of this law was the United Nations Modern Law on Electronic Commerce 1996. It was applicable to whole of India and to the persons of other countries also, if the crime involves a computer or network located in India.

This act classified the cybercrimes into following three groups:

- Cybercrime against individual includes
- Cybercrime against organization
- Cybercrime against Society

This act contains 94 sections, divided in 19 chapters and 4 schedules. IT act also amended various sections of Indian Penal Code 1860, India Evidence Act 1872, Bankers Book Evidence Code 1891, and Reserve Bank of India act 1934.

Information Technology Amendment Act 2008

The IT Amendment Act 2008 (ITAA) got the President assent on 5 Feb 2009 and was made effective from 27 October 2009 (Information Technology Act, 2000).

Some of the notable features of the ITAA are as follows:

- Introduced Section 66A as Publishing offensive, false or threatening information (imprisonment of 3 Years or Fine or both)
- Focussing on data privacy
- Focussing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cybercrimes like child pornography and cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

In March 2015, Honourable Supreme court declares the section 66A of IT Act, 2000 as unconstitutional and scrapped. The court said such a law hit at the root of liberty and freedom of expression, the two cardinal pillars of democracy. The court said the section has to be erased from the law books as it has gone much beyond the reasonable restrictions put by the Constitution on freedom of speech.

IT Act 2000 provided a legal framework for electronic governance by giving recognition to electronic records and digital signature. At the same time many experts of this field felt that the IT Act 2000 is (National Crime Records Bureau) not very effective in dealing with several emerging cybercrimes like cyber harassment, defamation, stalking and so on.

National Cyber Security Policy 2013

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology, Government of India. It protects the public and private infrastructure from cybercrime. It also protects personal information of internet user's financial and banking information.

Objectives of National Cyber Security Policy

1) To generate trust and confidence in all sectors of economy for enhancing adoption of IT.
2) To design new standard security policies.
3) To strengthen existing regulations.
4) To create a 24X7 mechanism to obtain information about threats to IT.
5) To improve and maintain the integrity of IT products and services.
6) By skill development and training, GOI wants to create a workforce of 5 lakhs professional
7) To reduce losses because of cybercrime & provide protection to privacy and information.

National Informatics Centre (NIC)

National Informatics Centre (NIC) is a premiere Science and Technology institution for providing e- governance solutions, adopting best practices, integrated services and global solutions in government sector. Information (National Cyber Security Policy 2013) is provided about activities of the Centre such as antivirus services, computer aided design (Cyber laws in India), geographical information systems, integrated network systems, internet data centre, IT training services, etc. Details of web services and web cast services are also provided.

4. Indian Computer Emergency Response Team (CERT-In)

The Indian Computer Emergency Response Team, under the Department of Information Technology of Ministry of Communications and Information Technology, works to enhance the security of India's communications and information infrastructure through proactive action and effective collaboration. It is a nodal agency that deals with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain.

In December 2013, CERT reported there was a rise in the cyber-attacks on Government organisations like banking and finance, oil and gas and emergency services. It issued a list of security guidelines to all critical departments.

Information Security Task Force (ISTF)

Since cybercrimes in India are increasing with a very fast pace, to combat the situation Government of India had set up an Inter Departmental Information Security Task Force (ISTF) with National Security Council (NSA) as the nodal agency (as per the report of Cyber Law and Information Technology by Talwant Singh, 2015) . The Task Force studied and deliberated on the issues such as

- National Information Security Threat Perceptions
- Critical Minimum Infrastructure to be protected
- Ways and means of ensuring Information Security including identification of relevant technologies
- Legal procedures required to ensure Information Security
- Awareness, Training and Research in Information Security

5. Challenges of Cybersecurity Policies of India

- **Lack of awareness**: India desperately need awareness of cybercrimes and the prevention approaches among their citizens, as India has very large number of internet users in the world.
- **Lack of a comprehensive policy**: IT Act of India is not sufficient to cover all the cybercrimes on its own. Although National Cyber Security Policy 2013 (NCSP) has implemented but it has come under criticism.
- **Government Policies are slow in using India's Talent**: India has a big pool of talent, but the government's policies are unable to exploit it.
- **Lack of a holistic approach**: India should involve the experts from the Information and Communication Technology field also rather than information technology alone.
- **Insufficient private sector inputs**: The policy formation process must include sufficient inputs from private sector as well including start firms.
- **Insufficient public input**: The policy formation process must include sufficient participation of civil society groups, RWA's, etc.
- **Lack of a security culture**: As per Internet World Stats Report, 2015 this is especially important in the cyber security domain, where every individual has the potential to be both a defender and a victim. India must therefore increase the priority it accords security issues in general.

6. Recommendations

- **India should use its large pool of available talent and capabilities.** As per Angshuman and Mondal Report 2015, India's significant talent and .capabilities in cyber security is one of its biggest strengths. With a highly educated, technologically skilled workforce, the country possesses one of the largest talent pools in the world.
- **An ideal blend of Western and Eastern approaches.** India has found an ideal blend of Western and Eastern approaches to cyber security. A per Srivastava and Ali 2015, the Western approach, led by the United States, looks at cyber security through a national security prism. The Eastern approach, driven by China and Russia, emphasizes social [22] cohesion.
- **Awareness programs**: India must run sufficient awareness programs, so that most of its citizens know about the cybercrimes and their prevention methods.
- **Increase punishment and Penalties**: India must make their penalties and punishment for cybercrimes as well as other crimes as hard as possible.
- **Cooperation**: Indian government should work cooperatively with industry and civil society groups to strengthen its legal framework for cybersecurity.

References

Angshuman A. and Mondal Kunal (2015) A survey of Indian Cybercrime and law and its prevention approach International Journal of Advanced Computer Technology (IJACT), VOLUME 1, NUMBER 2, pp-48-55,

Baylon Caroline (2014) Challenges at the intersection of Cybersecurity and space security, International Security: Country and International institution perspective, (Accessed on 1-12-2015).

Cyber laws in India, http://www.cyberlawsindia.net/ (Accessed on 4-12-2015).

Cyber Law and Information Technology, Talwant Singh, Addl. Distt. & Sessions Judge, Delhi http://www.slideshare.net/talwant/cyber-law-information-technology (Accessed on 5-12-2015).

https://en.wikipedia.org/wiki/Demographics_of_India (Accessed on 1-12-2015)

http://www.internetworldstats.com(Accessed on 2-12-2015)

http://ncrb.nic.in/ (Accessed on 1-12-2015)

http://www.cyberlawsindia.net/ (Accessed on 1-12-2015)

https://en.wikipedia.org/wiki/Information_Technology_Act,_2000 (Accessed on 2-12-2015)

https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013 (Accessed on 2-12-2015)

http://cis-india.org/internet-governance/cyber-crime-privacy (Accessed on 1-12-2015)
http://www.oxforddictionaries.com/definition/english/cyberterrorism (Accessed on 2-12-2015)
https://prezi.com/pq7inkjnx6bq/cyber-bullyingappropriate-use-of-media/ (Accessed on 2-12-2015)
http://india.gov.in/official-website-national-informatics-centre (Accessed on 3-12-2015)
https://en.wikipedia.org/wiki/Indian_Computer_Emergency_Response_Team (Accessed on 5-12-2015).
KPMG cybercrime survey report 2015,https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/Cyber-Crime-Survey-2015-30Nov15.pdf (Accessed on 3-12-2015).
Mittal Pradeep and Singh Amandeep(2013), *A study of cybercrimes and cyber laws in India*, SRJIS, Vol-1, Issue-1 (Accessed on 1-12-2015).
Poonia Ajeet Singh (2014), Cyber Crime: Challenges and its Classification International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 6, pp-119-121
Raghav S S (2015), Cyber security in India's counter terrorism strategy http://worldwidejournals.com/paripex/file.php?val=March_2016_1458622776__05.pdf (Accessed on 2-12-2015).
Seema S Shinde (2013), Cyber Ethics and Laws-Pros and Cons: A study of IT Act 2000, IJACEN, Vol-1, Issue-13 (Accessed on 16-6-2015).
Srivastav Abhishek, Ali Irman(2014), The Growing Phenomenon & Challenges of Cybercrime in India, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, pp 315-318
www.iibf.org.in/.../Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf (Accessed on 1-12-2015)