ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Studies Report on Cyber Law in India & Cybercrime Security

Anuraj Singh

MS Scholar, Dept. of M.S. Cyber Law & Information Security, Barkatullah University, Bhopal, M.P, India

ABSTRACT: Cyber law in India need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. Cybercrime is inescapable, ubiquitous and increasingly linked with different parts and areas of criminal environs. This evolution and network gave rise to cyber space which controls and manages to provide equal opportunities and facilities to all the people to access any kind of information. Due to gradually increase of the internet abusage of technology is broadening gradually which tends to cyber crimes. Cyber crime is basically an unlawful act that leads to criminal activity. Cyber Security, a mechanism by which computer information and the equipments are protected from unauthorized and illegal access. This paper illustrates and focuses on cybercrime, its impact on society, types of threats, and cyber security. Nowadays Computer crime issues and thefts have become tremendously high-profile, particularly those surrounding copyright infringement, hacking, child pornography, child grooming, and spoofing..

KEYWORDS: Cyber Laws in India, Cybercrime, Cyber security, Hackers, Fraud, and Privacy.

I. INTRODUCTION

Information technology is the new trick and Methodology of concept using computer and internet to retrieve, transmit, store, update, manipulate, and delete computer data or information, often in the context of business or other enterprises IT body. The Technology manly growth in 21st century saw a technological revaluation which enthralled not only India but the entire world. The use of computer is not limited to established institutions or organization, but available to every individual at the swipe of a finger. IT has eased out almost every humanized action. The unparalleled use of internet in our day-to-day lives also led to commencement of misuse of internet like data theft, illegal personal, and interference with privacy, cybercrimes.etc.

Computer fraud can be a untrustworthy misrepresentation of the fact proposed to prompt another to abstain from doing something that causes loss. Computer crime can be summarized as a criminal activity which involves information technology infrastructure, in addition to unauthorized access, illegal interception, any data interference, computer or systems interference, abusage of devices, forgery, blackmail, embezzlement, and some electronic fraud. There exits privacy issues whenever any confidential information or data is hijack or lost, either lawfully or otherwise.

Cyber crime cells are there in states basically to handle these crimes, and to expel or punish the netizens or criminals committing any of the cyber crime [1]. It basically ranges from theft of an individual's identity entire disruption of a particular country's Internet and network connectivity due to massive attacks across its networking resources. In this digital age, online communication now become a norm, the internet users and the government are at a enlarged risk of becoming the bull's-eye of the cyber attacks. Cyber crime can cause harm to any organization

Hacking of the ATM password, transferring the money by hacking the bank account details of the victim's account to theirs, some pornography issues etc are some of the thefts that are handled by educated people [2]. There is an urge to implement some of the rules and regulations, to tackle and handle these crimes governing cyber space particularly known as Cyber Law

Cyber security requires global co-operation to deal with the security of cyber space [3]. It protects computer equipments, resources of computer or system, information and data from any unauthorized access and the disclosure [1]. During this paper different kinds of attacks and threats are overviewed. Each and every attack is described firmly, category of hackers are also reviewed. In section II, cyber crime is detailed along with its two classifications of forms

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

of crimes. In section III different types of attacks are briefly overviewed. In the next section, section IV, category of hackers is acknowledged. Then cyber crime's impact is detailed in section V. Last section that is section VI, there is a short overview of cyber security is organized.

II. STUDY

Cyber Laws in India The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic 17 Commerce on International Trade Law.

Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives

Cyber law encompasses laws relating to –

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Information Technology Act, 2000

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government Information Technology Act, 2000 is India's mother legislation regulating these of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cyber crimes and liability of network service providers

Salient features of the Information Technology (Amendment) Act, 2008

The term 'digital signature' has been replaced with 'electronic signature' to make the Act more technology neutral. A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image. A new section has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public. New Section to address data protection and privacy -Section 43 Body corporate to implement best security practices-Sections 43A &72A

Applicability

Digital Signature under the IT Act, 2000

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Electronic Signature

Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule. An Amendment to the IT Act in 2008 introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

E-Governance

E-governance or Electronic Governance is dealt with under Sections 4 to 10A of the IT Act, 2000. It provides for legal recognition of electronic records and Electronic signature and also provides for legal recognition of contracts formed through electronic means. Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Controller of Certifying Authorities (CCA)

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA.

Penalties and Offences

Cyber Crime	Brief Description	Relevant Section in IT Act	Punishments
Cyber Stalking	Stealthily following a person, tracking his internet chats.	43, 65, 66	3 years, or with fine up to 2 lakh
Cyber Pornography including child pornography	Publishing Obscene in Electronic Form involving children	67, 67 (2)	10 years and with fine may extends to 10 lakh
Intellectual Property Crimes	Source Code Tampering, piracy, copyright infringement etc.	65	3 years, or with fine up to 2 lakh
Cyber Terrorism	Protection against cyber terrorism	69	Imprisonment for a term, may extend to 7 years
Cyber Hacking	Destruction, deletion, alteration, etc in a computer resources	66	3 years, or with fine up to 2 lakh
Phishing	Bank Financial Frauds in Electronic Banking	43, 65, 66	3 years, or with fine up to 2 lakh
Privacy	Unauthorized access to computer	43, 66, 67, 69, 72	2 years, or with fine upto 1 lakh

III. CYBERCRIME

Computer crime, cybercrime, electronic crime or hi-tech crime basically a criminal activity where a network or computer is the target, source, or place of the crime . Network crime encloses a wide range of illegally potential active activities. Whenever a person tries to steal information, or cause damage to computer network, this is assumed to be entirely virtual in which the particular information exists in digital form but the damage caused is real, which ceases the machine and has no physical consequence. A computer may act as a source of evidence, even though not directly or completely used for the criminal purposes, it acts as an excellent device for keeping the record and has given the in charge to encrypt data[5]. If the evidences are obtained and decrypted, it will be assumed to have a greater value to the criminal investigators. Generally, it is classified into two forms of categories:

1. Crimes targeting computer devices or network directly. Examples of crimes targeting computer devices or network directly would include,
   - Malicious and Malware code
   - Denial-of-service
   - Computing viruses
2. Prime target is independent of device or computer network.
   - Cyber stalking
   - Fraud and identity theft
   - Phishing scams
   - Information warfare

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

IV. THREATS TO BE AWARE OF

Denial-of-service It is an act in which criminal sends numerous spam mails to the victim's mail box depriving him/her of the entitled services to be provided. It is particularly an attempt to make the resources unavailable to users. Denial of Service (DoS) is basically produced by unintentional failure of nodes[10]. This attack is pervasive threat. The DoS attack attempts to exhausts the available resources by sending unnecessary packets to victim node. An attacker may take control of a system by taking the advantage of security weaknesses or vulnerabilities [6],[8]. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. We can follow these steps to reduce the possibilities that an attacker can make use of your system to attack other system:

1) Install anti-virus software.
2) Install a firewall to configure it and restrict traffic.
3) Follow remarkable security practices by applying email filters to manage unwanted emails.
4) Do not open email attachments, if they are from unknown people.

Malware is the most common way to infiltrate or harm your computer. The term malware is nothing more than "malicious software". Different malwares are Trojan, key loggers, spyware.

1) Alter files or delete them.
2) Intimidate you with scare ware.
3) Reformat hard drive causing you to lose all the useful information.
4) Steal some sensitive information.
5) Send emails using your identity.
6) Take charge of your system.

Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities. The process by which cyber criminals gain access to your computer. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware his computer is being accessed from a remote location. This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.

- Find weaknesses (or pre-existing bugs) in your security settings and exploit them in order to access your information.
- Install a Trojan horse, providing a back door for hackers to enter and search for your information.

Phishing is a crime mostly used by the criminals because it is one of the easiest ways to execute and it can produce the outcomes or results they're looking for with less effort. Websites, text messages, and fake emails are created to look as if they are from some authentic companies. Basically these are sent by some criminals to steal and acquire some personal and the financial information from you. This may also known as "Spoofing". Phishing is used by the strangers to "fish" or steal for information about you basically those that you would not disclose to a stranger, like your bank details, PIN, and some other personal details. What it does:

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Provides cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers

Spam is the method of both sending the information out and then collecting it from any unsuspecting people. Spam, an unlawful act or unsolicited sending of numerous amount of or bulk email for commercial purposes. The huge distribution of some unsolicited messages, pornography or advertising to addresses that are easily available and found on Internet through things example social networking sites, personal blogs, and company websites.

What it can do:

- Unwanted junk mails annoy you.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

- Phish for your data and information by tricking into some links or having details with soe very good and true offers and the promotions.
- Provide a vehicle for scams, malware, and fraud and threats to the privacy

Wormhole is basically a critical attack in which hacker or attacker records the bits or packets at a particular one location in the network and tunnels them to another one (location). In this attack, the malicious nodes eavesdrop packets and may tunnel the messages that are received in one area of network over some low latency link and finally retransmits them in some other. This may generate a false scenario representing the original sender in the neighbourhood of remote location. Basically tunnelling procedure outlines the wormholes in the sensor network. One can selectively proceed to the scenario of tunnelling or retransmitting of bits. Figure 2 demonstrates the wormhole attack in which the malicious node is "WH" which then creates the tunnel in between node „E" and node „I" because these two nodes are present at the most distances from each other. The easiest case of warm-hole attack is to basically have a malicious node which forwards the data in between the two legitimate nodes. Warm-hole attack can be launched by both the insiders and the outsiders.

Virus is the malicious and harmful computer programs that infect your system or may harm your contact list, are sent as an e-mail attachment basically and sometimes by downloading a file may also infect your system. Visiting a site sometimes starts an automatic download of a virus. They can send spam mails, may hijack your browser, sometimes disable the security settings and display unwanted and useful .They may also provide access of your system and contact lists to the criminals, and scan the personal information like bank account details, or passwords etc. When any of the programs might run, the viruses attached to that particular program could infiltrate the hard drive of the system and spread to the USB keys and also to the external hard drives. Now any attachment created by you using that particular program and sent to someone else may also infect them. Few things needs to be checked to know whether your system is infected or not

- It takes more than usual time to launch a particular program.
- Some Files and data get disappeared.
- Your system may crash constantly

Worms are basically a common form of threats that harms the computer or system or Internet as a whole. Unlike virus, worms directly attacks without any attachment of files, programs, images, text or something and works on its own. It resides in the memory of the system, doesn't cause harm to the hard drive and do not alter as well and propagates itself to other systems in a particular network. It may propagate by sending worm either within the company or to the internet itself. What they may do:

- They spread in your contact list.
- Tremendously causes damage by shutting down the parts of internet, and causes enormous amount of harm to the companies.
- Web pages now loaded slowly.
- Your system's screen looks like distorted.
- Programs run without any of your control

V. TYPES OF HACKERS

Any criminals or hackers are usually engineers, doctors, Non technical students etc all educated people who tries to gain the access of other's system. These are three type of hacker:

White Hat Hackers They are ethical hackers who basically focus on securing and protecting IT systems. White hat hackers are those who attempts to break into network or system in order to help the holder of the system by making an effort to aware them of the security flaws. Many such kind of people are employed by the companies concerning about the computer security; these are professional sneakers and the collective group of them are often categorized as tiger teams.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Black Hat Hackers An individual who compromises with the security of computer system without any acknowledgement from the authorized party. They uses their knowledge to exploit the systems.
Grey Hat Hackers A Grey Hat Hacker is considered as a skilled hacker in the security community who at times acts legally, and sometimes not. They are considered as hybrid between black and white hat hackers. They basically do not hack with the malicious intentions.

VI. CYBER CRIME IMPACT

Worms are the most strong form of cyber attack which causes severe disruption. In the month of September, in 2010, Stuxnet infected and affect the unknown number of industrial controls around the whole world, and stealthily give invalid instruction's to the machinery and some false readings to the operators . Potentially, it destroys gas pipelines, causes nuclear plant to malfunction or causes boilers of factory to explode. This worm was known to be active mostly in Iran, on the same Indonesia, Pakistan, India also reported as infections .
Crime Against People In this, the criminal provides numerous false promotions and gives the people an illusion of security by forcing them to administer their personal information. It includes child pornography, a dominant offence. Social networking sites and the chat groups can also be concluded as a serious cyber crime at times.
Crime Against Property Criminals can easily with their techniques steal the personal information of the other people computer system and the theft gains the unauthorized access to an internet connection, can be a cyber crime.
Crime Against Business In this crime, criminal basically hacks the system or machine of any business organization; they store and steal the confidential and the sensitive data of the system on the server. They acquire unauthorized access to the secured and confidential data of the company and via this, they transfer fund's of the company to their accounts that makes the organization bankrupt.
Crime Against Government Cyber terrorism is a term used against government crime in which hackers hacks the secured and confidential database of the government with the urge to use sensitive and personal information of the government that reduces the faith of the citizens.

VII. CYBER SECURITY

A branch of technology basically known as cyber security or information security applied to networks and computers, the objective carries protection of data or information and the property from the thefts, natural disaster, or corruption, and allowing the property and information to remain productive and accessible to its users .The Cyber security implies to the processes and the technologies which are designed to protect networks, computers and the data from the unauthorized access, attacks, and vulnerabilities delivered via the Internet by cyber criminals.

Prevention tips for cyber crime:

- Do Keep your firewalls (infrastructure defence systems) up to date.
- Make sure that your system is configured safely and securely.
- Always choose strong passwords and security checks for social networking sites, email boxes, and for your systems.
- Do not respond to unfamiliar mails.
- Protect your system with some security software
- Shield or protect your personal information from unknown people or strangers.
- Safe browsing, and do maintain some good system hygiene.
- Keep updating your passwords, and login id's at least once or twice in one or two months and make them strong.
- Do protect your data and personal information and avoid being scammed.
- Never send personal information and data via mail or any other means.
- Make your system clean time to time and review your social media sites as well.
- Do not respond to any spam email and be cautious

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

VIII. CONCLUSION

In this modern of technology Indian cyber law, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cyber criminals to access any data and information with the help of their knowledge and their expertise. Cyber crime is an unlawful act or a menace that needs to be tackled firmly and effectively. There is a need to create more awareness among the people and basically users of internet about cyber space, diverse forms of cyber crime and some preventive measures as "Prevention is always better than cure", so it is seriously advised to take some previous precautions while operating the internet. Security nowadays is becoming a prominent and major concern. In the following paper, some IT Law & security issues are introduced, threats, Trojans, and attacks over internet. Computer security becomes critical in many of the technology-driven industries which operate on the computer systems. Computer security is nothing more than computer safety. Countless vulnerabilities and computer or network based issues are acts as an integral part of maintaining an operational industry.

REFERENCES

1. Cyber Crime Investigation Field Guide – By Bruce Middleton.
2. Cyber Crime – By R K. Suri. & T N. Chhabra**.**
3. *http://catindia.gov.in/Default.aspx* -Cyber Appellate Tribunal
4. *http://www.cert-in.org.in/* -Indian Computer Emergency Response Team
5. *http://cca.gov.in/rw/pages/index.en.do* -Controller of Certifying Authorities
6. Research paper of Cyber Crime and Security Soumya Tiwari* , Anshika Bhalla, Ritu Rawat
7. http://www.ssrana.in/Intellectual%20Property/Information%20Technology%20Law/Information-Technology-Law-in-India.aspx S.S Rana & Co. Advocates
8. http://www.cyberlawsindia.net/cyber-india.html
9. Pooja Aggarwal , Neha, Piyush Arora , Poonam , "REVIEW ON CYBER CRIME AND SECURITY", IJREAS, Vol. 02, Issue 01, Jan 2014.
10. Ammar Yassir and Smitha Nayak, "Cybercrime: A threat to Network Security", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012.
11. Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, "Cyber security: challenges for society- literature review", IOSR Journal of Computer Engineering (IOSR-JCE) , Volume 12, Issue 2 (May. - Jun. 2013), PP 67- 75.
12. A. T. Zia, "A Security Framework for Wireless Sensor Networks". 2008, http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf.
13. en.wikipedia.org/wiki/Cyber_security_standards.