A Study on Emerging Issues of Cyber Attacks & Security: In India

Submitted by:

ADITI SINGH

Amity Law School, Noida

B.A., LL.B (H) 2nd Year, 4th Semester

ABSTRACT

In the digital age, data plays a huge role in our ordinary lives. It's present in lots of evident ways. The digital world has transformed our lives creating new ways of communicating, organizing and accessing information. It has also generated new threats popularly known as 'cyber crimes' which are increasing tremendously day by day. In response cyberspace is increasingly being framed as something inherently dangerous. Which require more scrutiny management and control. Besides various measures cyber security is still a major concern to many. Securing the data have become the biggest challenge in the today's society where internet is easily available. This paper will explore why this framing is itself a threat to both human rights and the security of the digital environment. By the end it will help in understanding the dominant ways threats in cyberspace are being framed. Why this framing can be problematic and how to get involved it these debates. This paper aims to identify how we can engage with Government and Citizen to protect and strengthen these rights. It also focus on modern techniques and ethics in changing the face of cyber security.

***KEY WORDS**: Cyber Security, Cyber Crime, Cyber Ethics, Cyber Space, Data, Digital, Social Media, Government.*

I. INTRODUCTION

The word Cyber originally came from Cybernetics derived from the Greek kubernētēs which refers to a Pilot or steersman. [1] It was actually popularized by an American mathematician Norbert Wiener. He wrote a book in the 1940's called Cybernetics. This was his prediction for a future which is dominated by a self-governed PC framework that had its own feedback loop and would continue to grow. It wasn't actually until the 1980's when cyber linked with other words meaning something related to digital. Cyber is "relating to or characteristic of information technology, virtual reality or computers." If we mention that today we live in a Cyber age, it means the age of analysts, virtual reality, or information technology. Just like real universe cyber universe is expanding. In last 60 seconds for instance there will have been thousands and millions of updates on Facebook, twitter and on other platforms. We spend our time on checking emails every day. There are estimates that over 70% of those emails are actually spam or hackers or spam in terms of malicious software trying to gain access to your systems and to your personal information.

A Cyber Attack occurs when hackers try to destroy or damage a computer system or network. Cyber Space is the notional environment where communication over computer network happens. Initially, the term entered popular culture from science fiction. Today, however, many people, including technology strategists, industry leaders, security professionals, and the military use it. We use cyber space to describe the domain of the worldwide technology environment.

The development of technology has made man reliant on Internet for all his needs and it is affecting us an individual and as a society. It has given man simple access to everything while at the same time sitting at one spot. Whether it's about Social networking, web based shopping, data storage, gaming, online classes, online job opportunities, each conceivable thing that man can consider is achievable with the help of Internet. It is utilized and consumed in every possible way. With the enhancement of the web and its related advantages likewise built up the idea of cyber-crimes. When the Internet was first created the founding fathers had absolutely no idea that the Internet could be misused by criminal activity. A couple of years back, there was lack of awareness about

the violations that could be committed through web. With the rise of the innovation the abuse of the innovation has equally extended to its ideal level. Since the turn of the century, cybercrime has increased dramatically. Cybercrimes may threaten a country's security, an entity's financial health or even an individual. India is similarly not far behind different nations where the pace of occurrence of digital violations is increasing day by day.

II. OBJECTIVE OF STUDY

- To comprehend what nature of Cyber-attack occur in our country.
- To understand the Cyber Security Techniqueswhich can be used stop such malicious activities from rising.
- To seehow one can make sure about his Privacy and Personal information and keep oneself from turning into a survivor of cyber-crime.

III. LITERATURE REVIEW

Some of relevant literature surveys are discussed here:

i. A report from Symantec Corp. (presently part of Broadcom) a year ago uncovered that India is the second most cyber attacked nation on the planet, after the U.S. and China. This was generally announced in the media. Indian law, prominently the Indian IT Act 2000, doesn't completely shield its residents from new attack vectors like phishing, SIM jacking, ransom ware, mobile instalments fraud, bank fraud, malware assaults, social building, and DDoS attacks all inexorably regular nowadays.[2]

ii. Das (2013) He discusses that the effectiveness of the Internet has proved itself in numerous and countless ways that will hopefully be enough to make sure it does not become a wasteland of criminal action and a upholder for the malicious. According to him government will have to huge role but most of the prevention needs to be handled by commercial entities by producing software which have the ability to stop frauds.[3]

IV. RESEARCH METHODOLOGY

A Research Method denotes the technical steps involved in writing the research. The research is done on "Study on Emerging Issues of Cyber Attacks & Security: In India" The Quantitative Research Design used is in this paper is Descriptive research. Descriptive research elaborate the current status of an identified variable. These research are intended to provide systematic information about an issue. Systematic collection of data requires careful selection of the topics studied and careful measurement of every factor. The Data Collection Technique used in this research paper involves the collection of data from Secondary Sources I.e. Articles, Books and Websites.

V. CYBER CRIME

We can define "Cyber Crime" as any malefactor or other offences where electronic communications or information systems, including any device or the web or both or more of them are involved [4].

Cybercrime is a crime that includes a framework (system) and a network. The computer may have been utilized in the commission of the crime, or it might be the object or target. Digital crimes are offenses that are enacted against a person or persons, with criminal intent, which purposely damages the victim's reputation or causes direct or indirect physical or psychological harm to the victim using modern telecommunications. For example, Web chat rooms, cell phones, messages or emails and notice feeds. Such crimes pose a threat to the country's security and economic health. Issues including these sorts of crimes have a high profile, especially those encompassing hacking, copyright infringement, child pornography. There are additional issues of security when secret data is blocked or uncovered, legally or otherwise. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cybercrimes.

Cyber Crimes can be mainly divided into 3 major classifications:

- Cyber Crimes against persons
- Cyber Crimes against property
- Cyber Crimes against government

- **Cyber Crimes against Persons-** Cybercrimes against individuals include various offenses such as the transmission of Child pornography and the harassment of anyone with the use of PCs such as e-mail. Dealing, circulation, posting and distribution of obscene material including pornography and indecent public nudity is one among the foremost important Cybercrime known today. The harm done to humanity by such crimes is not great. This is cybercrime, which threatens to undermine the development of the younger generation, as it leaves irreparable scars and wounds on the younger generation if it is not controlled.

  Cyber harassment is a separate cybercrime. Various forms of harassment can and do occur in cyberspace or through the use of cyberspace. Harassment can be sexual, racial, religious or otherwise. People perpetuating such harassment are also committing cybercrimes.

  Cyberbullying can also bring crime to another related area that violates the privacy of citizens. Violating the privacy of online citizens is a serious cybercrime. Nobody likes being attacked by other person on the invaluable and most poignant part of their privacy, which grants citizens over the Internet.

- **Cyber Crimes against Property** - The second classification of Cyber-attack is that of Cybercrimes against all types of property. Crime incorporate PC vandalism (destruction of other's property), transmission of damaging programmes, siphoning of assets from financial foundations, stealing undisclosed data and information.

  A Mumbai-based start-up organization lost a lot of cash in the business when the opponent organization, an industry major, took the technical database from their PCs with the assistance of a corporate cyber spy.

- **Cyber Crimes against Government** - The expansion of web has indicated that the mechanism of Cyberspace is being utilized by people and groups to threaten the international governments and additionally to threaten the residents of a nation. This crime manifests itself into terrorism when an individual "crashes" into an administration, state or military maintained website.

VI. CYBER CRIME IN INDIA

The Internet Crime Report for 2019, discharged by Unites states Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation, has broadcasted that India stands third on the globe among top 20 nations that are victims of cybercrimes. According to the report, excluding the USA, the United Kingdom best the rundown with 93,796 casualties of cybercrimes followed by Canada (3,721) and India (2,901).

As per the most recent National Crime Records Bureau (NCRB) information, a total of 27,248 instances of Cyber-attack were enlisted in India in 2018. In Telangana, 1,205 cyber-attack cases were enrolled around the same time. The National Cyber Crime Reporting Portal that was begun a year ago by the Central government got 33,152 grievances till now, bringing about lodging of 790 FIRs. [5]

Cyber Crime is not only covered under IT Act. Some provisions are under the Indian Penal Code too.

Following are the few examples of Cybercrime in India:

i. **E-Mail Bomb**: It's a type of Internet misuse which is executed and involves sending large amounts of emails to a particular email address with the objective of flooding the mail box and overpowering the mail server facilitating the address and crashing the service.

ii. **Hacking**: Hacking is an attempt to misuse a PC framework or a private network within a PC. Basically, it is the unapproved access to or power over PC security frameworks for some illegal motive. It's done by hackers who are highly skilled in breaking a security system.

iii. **Spreading computer virus**: A PC infection, it's a malicious program design (i.e. destroying data) stacked onto a client's PC without the client's information and performs malevolent activities. It can spread through E mails, Pen drives (secondary storage), Multimedia and Web.

iv. **Phishing**: Phishing is a cybercrime wherein an objective or targets are reached by e-mail, phone or instant message by somebody acting like an authentic establishment to draw people into giving delicate information, for example, recognizable data, banking, credit card details and passwords. This data is then used to get to significant records and can bring about extensive fraud, identity theft and monetary loss.

v. **Identity theft:** Identity theft is the obtaining of another person's private or financial data for the only purpose of transacting or buying through that person's name or identity. It includes getting access to corporate databases to steal lists of client data and destroying their private and credit data.That criminal shall be punished with imprisonment of either description for a term which may reach three years and shall even be subject to fine which may reach rupees one lakh.

VII. CYBER SECURITY

A hospital's patient data is leaked, power system is hacked, and comments insulting a political leader is posted on a social media network. These scenario might seem different, but they could all come under the banner of cyber security. Government and businesses in particular tend to frame cyber security

Cyber security is defined as a techniques and practices designed to protect data. It applies to the Digital Data. Data that is stored, transmitted, in use on an information network, server or system.Information is the lifeblood of cyberspace. From personal data to high- level state communication it flows through networks in huge quantities and is stored on devices and data centres. We can't talk about cyber security without mentioning about technology.

The IT Act, 2000 characterizes "cyber-security" as the insurance given to devices and information stored therein from "unauthorized access, use, disclosure, disruption, modification or destruction."

Government institutions and regulation for cyber security:

1) **The National Technical Research Organization** is the main agency designed to protect national critical infrastructure and to handle all the cyber security incidents in critical sectors of the country.

2) **The Indian Computer Emergency Response Team** is at liable for responses including examination, forecasts and cautions on cyber security issues and breaks.

CYBER SECURITY TECHNIQUES

1. **Strong Password Security**: Using a strong and complicated password is an easiest task to upgrade the security of your system. E.g. Password which uses special characters, numbers and letters. Regularly updating it can help stop brute force password cracking.
2. **Authentication of knowledge**: **Regular update and Using with caution:** Programmers (hackers) can abuse an email and web in numerous way, use it with caution.Updating system and periodic backup programme is an incredible method to guarantee your information is retrievable and protect and repair any bugs or defects with the system.
3. **Malware scanners**- Software which tests malicious code in addition harmful viruses in all files present in the device. Viruses, worms, and Trojan horses are samples of malicious software that are often clustered together and known as malware.
4. **Firewalls**- A software program or part of hardware which helps sort hackers, viruses, and worms that attempt to reach your device over the web. All messages incoming or leaving the web undergo the firewall present, which examines each message and blocks the one against required safetystandards.
5. **Anti-virus software** -Installing anti-virus software is a vital step to protect your PC network from viruses. It vigorously scans your emails, system documents from viruses that come into your operating system. A good anti-virus implements periodic updates and should be compatible with system.

VIII. CASE STUDY

Andhra Pradesh Tax Case [6]

In Andhra Pradesh, the owner of a plastic company was taken into custody. The Vigilance Department recovered Twenty-Two Crore of cash from his home. They wanted details and justification from the person regarding to the unaccounted cash. The accused person deposited 6,000 vouchers to validate the authenticity of the business. But after a vigilant examination of the vouchers and data in his PCs, it was revealed that all the vouchers were made after the raids were conducted. It was found that five businesses were running in the presence of one company and the alleged used fake and computerized vouchers to show sales records and save tax. As a result, the questioning strategies of the Andhra Pradesh chief businessman appeared as the department officials confiscated the computers used by the accused.

The Bank NSP Case [7]

The case of Bank NSP is that where the Bank Management Trainee was engaged and was getting married. The couple exchanged numerous e-mails and messages and used the company's PC. After some time the two parted away and the young lady created deceitful email Ids by name "Indian Bar Associations" and sent mails to the man's foreign customers. She used the bank's PC to do this. The man's company lost many customers and took the bank to the court for the loss. The bank was responsible and was held liable for the e-mails sent using the Bank's system/ PC.

State of Tamil Nadu vs.SuhasKatti [8]

This case is linked with posting of explicit, defamatory and frustrating message about a divorcee lady in the yahoo texting group. E-Mails were additionally sent to the victim for evidence by the alleged through a wrong e-mail account opened by him within the name of the victim. The posting of the message resulted in annoying phone calls to the lady within the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within subsequent few days. The accused was a known family friend of the victim and was reportedly curious about marrying her. She however married another person. This marriage later led to divorce and therefore the accused started contacting her once more. On her reluctance to marry him, the accused took up the harassment through the web. On the prosecution side 12 witnesses were examined and full documents were marked as Exhibits. The court depended upon the expert witnesses and other proof produced before it, including witnesses of the Cyber Cafe owners and came to the decision that the crime was conclusively proved and convicted the accused. This is considered as the first case in Tamil Nadu, in which the offender was convicted under section 67 of IT Act in India.

Online Credit Card Fraud on e-Bay [9]

Rourkela police bust a racket including an online fraudvalue RS. 12.5 lakh. The "modus operandi"of the accused was to hack into the eBay India site and make buys in the names of credit cardholders. Two individuals, including suspected mastermindDebasisPandit, a BCA student, were captured and sent to the court of the sub divisional judicial magistrate - Rourkela. The other captured individual is Rabi Narayan Sahu. A case has been recorded against the blamed under Sections 420 and 34 for the Indian Penal Code and Section 66 of the IT Act. DebasisPandit purportedly hacked into the eBay India site and accumulated the details of around 700 credit cardholders. He at that point made buys by using their passwords. The fraud went to the notice of eBay authorities when it was identified that few buys were done from Rourkela while the clients were situated in cities, for example, Bangalore, Baroda and Jaipur and even London. The company carried the issue to the notice of Rourkela police after certain clients lodged complaints.

IX. CYBER ETHICS AND PRACTICES FOR PREVENTION OF CYBER ATTACK

It refers to the code of responsible behaviour on the internet.
The fundamental guideline is try not to accomplish something in cyber space that you would consider wrong or illegal. [10]

1. Do utilize the internet to covey and interact with others. Email and texting helps in keeping contacts with family, friends, colleagues. Sharing new concepts, thoughts and information with individuals across the city or around the world.
2. Never share or send your personal data like bank account no., password, ATM pin and so on over an unencrypted network including unencrypted mail. Sites that doesn't have lock icon and https on the

address bar of the browser are the decoded site. The "s" stands for secure and it demonstrate that the site is secure and safe.

3. Never sign to any social networking platform and sites until it's legit and authentic.
4. Never forget to refresh and update the operating framework. Software like Firewalls, anti-virus and anti-spyware programming should be installed and frequently updated in ones PCs.
5. Never visit,follow and respond to spam and un-trusted website or link.
6. Don't be a harasser or a bully on the Internet. Don't use offensive languages or comments. Do not call people names, defame them, send embarrassing and explicit pictures of them, or attempt to hurt them.
7. Web is considered to be world's largest library with information on any theme in any branch of knowledge. So use this data in a right and legal manner.
8. Never share your password with anyone and never operate others account by using their passwords.
9. Never share your personal data to anyone as there is a decent possibility of others misusing it and you will have to face the consequences.
10. Never click on pop-ups that offers site survey or study on ecommerce websites or any other site as in some cases it comes with malicious software. When we acknowledge or follow pop-ups a download is performed in the background and that file contains the malware and malicious code and it known as drive-by-download.
11. Always cling to copyrighted data and download games or recordings only if they are admissible.
12. Never attempt to send any sort of malware to other's PCs and make them corrupt.
13. Never fake your identity and create fake accounts of other persons as it would land you and the other individual in trouble.

The above are some Cyber Morals one must follow while utilizing the web. We apply some appropriate principles and conducts in our lives from very early stages same we apply in this Cyber world.

X. CONCLUSION

A country with 1.3 billion people, INDIA with the lowest data charges in the world. Securing data and information is becoming more important with the advancing network. This study clears that with the development of cyberspace and technology the scope of cyber threats will increase too. One must use Cyber security measures like using firewalls, keeping strong passwords, installing antivirus and should practise prevention of cyber-attack to protect data. India's reactive approach of protecting cyber system only after being dictated by occurrence of cyber security cases needs to be change into proactive one. As it is the need of the hour. Awareness, Firm amendments, penal provision and cyber security policy are needed in order to protect rights and privacy in order to uphold rule of law.

REFERENCES

[1] https://alpinesecurity.com/blog(Visited on 18th April, 2020)

[2]https://www.cisomag.com/india-cybersecurity-policy/(Visited on 21st April, 2020)

[3]Sumanjit Das and TapaswiniNayak, "IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES" 6 IJESET 142-153 (2013).

[4]https://cybercrime.org.za/definition(Visited on 24th April, 2020)

[5]https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (Visited on 25th April, 2020)

[6]https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf(Visited on 27th April, 2020)

[7]https://www.cyberralegalservices.com/detail-casestudies.php(Visited on 2nd May, 2020)

[8]http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html (Visited on 6th May, 2020)

[9] Puja Gupta and Rakesh Kumar, "Security Risk Management with Networked Information System: A Review"4 (2) IJEE193– 197 (2012).

[10] VeenooUpadhyay, Dr.SuryakantYadav, **"**Study of Cyber Security Challenges Its Emerging Trends: Current Technologies"5 IJERM 2349-2058 (2018).