Cyber Security: Issues Relating To Cyber Crime

Cyber Security

“It’s only when you go wrong that machines remind you how strong they are”- Clive James

Introduction

Internet as the global network was introduced to make the lives easier and faster. But who knew that would come with whole lot of faults. One such defect of this was its overuse and crime that followed it. As the technology continues to evolve so do the society has to face the opportunities and challenges that it throws on us. And likewise just as the technology brings with it, its battens so does it brings with the menace of cyber crime, cyber attack and industrial espionage. Recently a case happened to be in Pune, India, where the hackers used an unidentified malware function to attack the server of Pune based Cosmos Bank. They cloned thousands of bank’s debit cards and debited an amount of almost 93 crores. The cloned cards were of Visa and Rupay. The absurd use of this has caused to put our lives on show. Talking about this the one word ‘cyber’ has gradually entrenched into our daily lives and discussions. Out of all the crimes penetrating in the society the one that has completely propagated its threat into people’s mind is the cyber crime. When every now and then you read about the articles of an unknown username making millions by leaking the web passwords of vulnerable people is because of the lack of awareness among them about the cyber security, its advantages, procedures and uses. Also when we talk about the victims of the cybercrime, there’s also an absence of knowledge about seeking remedies from legal systems.

What Is Cyber Crime?

Cybercrimes also known as computer-oriented crimes are basically the crimes that are intended towards an individual or group of individuals to defame them or harm them either mentally or physically or cause loss to them. The victims could be attacked directly or indirectly through cloning their telecommunication devices. Threatening through cyber crime could be to either a person or a nation which would harm its security or financial health. Of course the crime has gone to heights as the people are using or may be carelessly using the technology. Yes the criminals are to be blamed for the crime they do but don’t you think that it’s our fault too that we don’t use the technology wisely. The propagation of internet is so fast and wide that we at times forget is cons. It is our careless attitude sometimes that they get an opportunity to take benefit of our lives. The Black’s Law Dictionary explains the term privacy as being free from intrusion of public attention with a person’s acts of intentions. And the technology very easily gives access of your privacy to the people who wrongfully use it against you without even your consent. There is a certain way that the cybercriminals work in. It has made its way from a bedroom-bound geek to a whole chain of gangsters working through and channeling it. The groups are mostly associated to crimes like hacking, sextortion, child pornography, copyright infringement etc. are all issues that are highlighted to a level but could not be stopped from elevating.

Issues Relating To Cyber Crime

There are certain issues relating to the cybercrime that are increasing on a daily basis:

1. Sextortion- As the young generation gets more and more accessible to the social media they tend to use it in a more absurd way and create sexual content and gets viral online. The risk of online sexual bullying and it's live streaming increases. It's important that we make the younger's aware about the pros and cons of internet and social media before they are exposed to the virtual world.
2. Hacking- It is the invasion into someone's private data without their permission. Access to their personal data is basically called hacking. Now there are 3 types of hackers:
    1. i) White hat hackers: They are the people who believe that hacking one's system and sharing its information with a good intention is right to do.
    2. ii) Black hat hackers: They are the professionals who invade into your data and steal them or corrupt it by inserting viruse4s into them. They are also called the crackers.
    3. iii) Grey hat hackers: They are4 basically the hackers that are ethical but often would unethically hack your systems to spread some kind of information for just fun or their curiosity.
3. Cyber stalking- It is an activity where the stalker detects the information of a person from an online platform to stalk their daily activity.
4. Spamming- Sending unwanted messages or advertisements into your mailing box to overload your system with uncalled for data is called as spamming.
5. Cyber pornography- This is a situation where mostly the women and children are sexually exploited. Pictures and videos in an exploitative way are shared and made viral.
6. Software piracy- It is usually intrusion into private data of some company for the business purpose or for individual use. It is somewhere related to the business of copyrights.
7. Cyber terrorism- when the computer systems and the internet are used to threaten the government, the civilians or a group for the terrorist attacks in the area is called cyber terrorism. Even at times these terrorist blackmail people by hacking their systems and exploit the anonymous to threaten the government.

Statistical Data

Today we are more and more dependent on technology that could be hacked easily. And there are some of the most shocking analytical data about the cybercrime. It has been stated that every 39 second there takes place a hacker attack, over 24,000 apps are blocked everyday that are malicious in nature, 21% of the files in the world that contain credit card records, personal information and health records aren't protected.

1. The research of 2018 states that almost 700 billion people were victim of cyber crime that year. That was because almost 20 countries had outdated laws or no cyber laws.
2. The stereotypical mom's basement industry that has now become a hub of professionalism generates almost $1.5 trillion annually out of the cyber crime.
3. Not only the natural citizens but also the companies face the issues relating the hackers and the cyber crime. Almost 16,500 times is no. of attacks that companies face in a year. This not only drains in money in the lawsuits but also affect their client trust.

4. $172 billion or $142 every person is the average amount of money that has been lost by the victims of cyber crime in the year 2017.
5. It is expected that the rate of cyber crime shall quadruple by the year 2021 and would cost about $6 trillion.

As for talking about just our nation the rate of cybercrime has reportedly increased about 19 times in about 10 years, 2005-2014. Also India is ranked at third position as a source of ‘malicious activity’ and at second position for creating ‘malicious code’.

Aren’t these figures horrifying? Are we not supposed to get more serious about the business? Shouldn’t we be more careful about the devices that we use? These are some of the unanswered question that should be answered as soon as possible.

Cyber Security

Cyber security is a way which one could protect its personal data against the unauthorized and malfunctioned interruption and also theft of your virtual belongings. It is for defending your devices from getting hacked and exploited. Cyber security is well designed computer programs that are important for mobiles, computers, programs and networks. Cyber security is needed for everybody from a layman to big institutions like corporate and government institutions like defense and finance where the data is confidential and even a small amount of negligence could cause harm to nation’s security. Cyber security is basically aiming at accessing, changing and destroying the networks and databases of the system which have been attacked by hackers or more less the cyber criminals. It is very important that we pay attention to this topic because we can be smart and innovative enough but we need to understand that hackers today are even two steps ahead. The cyber security majorly deals with the technology, the people who use the technology and the processes of technology. Now, for technology it is important that with advancement in the technology there be an up gradation in the security. For the people who use the technology its necessary that people are made aware the cyber security and its advantages. As the global connectivity is increasing and the use of cloud services hype it is important that we encompass our sensitive data and personal information from theft and hacking for malfunction. There’s nothing that we don’t use the internet for- from entertainment to communication to banking and what not. Cyber security holds its importance because the big institutions like the government or the military or the medical and financial institutions store some the most confidential databases disclosing of which could cause harm to the security of the nation as well. Even if the data is hacked from natural man’s device it could be used against them and threaten them for the wrong. There are certain types of security. The five main of which are:

1. Critical Infrastructure security- this type of security is used and should be used in places like shopping centres, hospitals, electricity grids etc. looking at their vulnerability.
2. Application security- It is a general form of security for the programs of devices by using hardware and software at the time of development of the program. Some of them are like antivirus, firewalls etc.
3. Network security- it is a type of security that protects your device from malicious content that interrupt your work.
4. Cloud security- Cloud security is a software-based program that protects your cloud resources from malfunctioning. Also it is because cloud has taken over the security

services that it has become more reliable.
5. Internet of things (IOT) security- It refers to a wide variety of significant and non-significant physical cyber-physical systems like security cameras, wifi- routers, printers etc.

Laws Relating To Cyber Crime In India

IT revolution started in India under the tutelage of then Prime Minister Rajeev Gandhi but the Information Technology Act, 2000 came into existence on 9 May 2000. The original act consisted of 94 sections divided into 13 chapters and schedules. The Indian Information Technology Act 2000 is based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. As of 2017 7.4 billion people are using internet that is half of the Global population. This technology has been used in not only creating millions of jobs what is proving to be a lifesaver. But, there are certain anomalies which can't be ignored. Even though the vision was to help humanity, has become the new hub of international crimes. Its waiting anonymous nature has given the internet criminals a new Breeze of life virtual ghost. Hence, code of regulation was the hour of need. India, being at the forefront of the Earth revolution rested no time and table in information technology act 2000 objectives.

1. To save the critical information which are of national interest being leaked into the wrong hands?
2. To protect the dignity of human lives it was necessary to stand in the laws relating to privacy.
3. To ensure that the children are safe from prying eyes.
4. To ensure that there is necessary infrastructure to secure the servers.

Following are some of the important sections of the IT Act, 2000:

1. Trying to tamper with computer resources- Section 65
2. Trying to hack into the data stored in the computer – Section 66
3. Provision of penalties for misappropriation of information stolen from computer or any other electronic gadget – Section 66B
4. Provision of penalties for stealing someone’s identity-Section 66C
5. Provision of penalties for access to personal data of someone with the help of computer by concealing their identity- Section 66D
6. Provision of penalties for breach of privacy- Section 66E
7. Provision of penalties for cyber terrorism- Section 66F
8. Provisions related to the publication of offensive information-Section 67
9. Provision of penalties for publishing or circulating sex or pornographic information through electronic means- Section 67A
10. Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode – Section 67B
11. Provision of penalties for disrupting or blocking information by mediators- Section 67C
12. Provision for making objectionable access to a secured computer-Section 70
13. Delivering data or data incorrectly – Section 71
14. Provisions related to mutual trust and privacy – Section 72
15. The provisions relating to making public the information violation of the terms of the Protocol- Section 72

16. Publication of Ezra Digital Signature- Section 73

Also the Ministry of Electronics and Information technology introduced the Personal Data Protection Bill, 2018 under the chairmanship of Justice B.N.Srikrishna. It deals with transfer of data with consent. It states that with every transfer of personal data you need the consent of the same person.

Landmark Cases Of Information Technology Act, 2000

· Shreya Sighal V Union Of India Writ Petition (Criminal) No.167 Of 2012

Shreya Singhal v. Union of India is a judgement by a two-judge bench of the Supreme Court of India in 2015, regarding the issue of online speech in India. The Supreme Court struck down Section 66A of the IT Act, 2000 relating to restrictions on online speech, as unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the constitution of India.

· Sharat Babu Digumarti V State, Government Of Nct, Delhi Criminal Appeal No. 1222 Of 2016 (Arising Out Of S.L.P. (Criminal) No. 7675 Of 2015)

Appellant was the director of a company and was charged under section 292, 294 IPC r/w section 67 of IT Act, 2000. He was accused of possessing and selling and distributing it. Proceedings under the IT Act were dropped but the court was of the opinion to solely continue the proceeding on Section 292 of IPC. The issue was whether the IT Act 2000 will override the provisions of IPC. The court held that section 67, 67,67B clearly stipulate the punishment for publishing, translating option material in electronic forms. Section 292 of IPC also prohibits the selling of obscene books. That both offences are similar, the court held that the law having an overriding effect will prevail.

· Kent Ro Systems Ltd And Anr V Amit Kotak And Ors Cs(Comm) 1655/2016 & Ia No.15914/2016

Court held that hosting of information on e-commerce websites is automatic and it is not expected of the website to screen each and every piece of information except when the same is brought to it’s knowledge. Therefore, to require an intermediary to do such screening would be an unreasonable interference with the rights of the intermediary to carry on its business.

· Mohammad V State (2010)

Section 67 of Information Technology Act analyzed and held it is not applicable to the case of threatening email received by Chief Minster of Gujarat, hence ordered to be deleted from the matter.

· Vyakti Vikas Kendra And Ors V Jitender Bagga And Google (2012)

Art of Living Foundation filed for interim relief against a blogger and the intermediary Google owned Blogger.com for cyber defamation. The latter was ordered to remove all the defamatory

content within 36 hours

· K. Ramajayam V The Inspector Of Police (Criminal Appeal No.110 Of 2015)

If an electronic record as such is used as primary evidence under Section 62 of the Indian Evidence Act, 1872 the same is admissible in evidence, without compliance with the conditions in Section 65B of the Evidence Act.

· Suhas Katti V State Of Tamil Nadu,2004

This was the first ever case where the accused in the case of cyber pornography. The court held Katti under sec. 469 of IPC with two years of rigorous imprisonment and fine of rupees500/- and under sec. 509 of IPC with two years of rigorous imprisonment and rupees4000/- fine for the offence under sec. 67 of IT Act, 2000 which states punishment for publishing or transmitting obscene material in electronic form.

Conclusion

Cyber security has become the need of the hour and it has now become a necessity that we understand this need. Cyber technologies have given criminals a well made platform to commit crime in an easier way. And we have become to understand the potential and value of human security. The surfeit of human security is not new but definitely ignored. And it’s high time we pay the much needed attention to it. The issue of cyber security is the root cause of many other criminal activities. And to fight with those we have to make people aware about it also about the remedies that they could seek legally from the statutory bodies. The growth of cyber crime in India and internationally is at height. And most of the crimes are either related to women who are active on internet or it’s a threat to the governmental bodies mostly. The IT Act, 2000 and provisions of Indian Penal Code, 1986 are all limited. They are limited and needed to be enhanced. Also more cyber cells are needed to make so that people get speedy trials and justice.