INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 2 | Issue 3

2020

Cyber Security and Digitalisation

MILIND JAIN[1]

ABSTRACT

The most common question that arises between us is that what is Cyber Security and why do we need rules and regulations for that?. Now Cyber Security simply means the protection of data for an Individual's interest or in the Interest of State. There are many viruses and invaders that wants to invade our privacy and attack on us for that there is one law which is known as Cyber Law, and that Cyber Law talks about how we need to pay attention in the virtual world. The need for Cyber Security is to protect our won personal data from the outside world, as we have seen so much online scams going on in this daily world and specially in India. Many of the youngsters or Teenagers are used to use many such online chat platforms in which at any time the chats or any talks can be taken out. So for protection of those we need Cyber Security.

In this paper author will be dealing with What is Cyber Law, What is Cyber Security, What is the situation of India in dealing with such crimes, how many cyber-attacks have been taken place with the help of some cases, need for cyber security in India and last but not the least what is the legal framework of out Judicial System in dealing with such crimes and what are the steps taken by the Government of India in dealing with such crimes and situations.

I. INTRODUCTION

The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic."

— Stephane Nappo

To understand what Cyber Security is, first we need to know about what is Cyber law so that we can understand Cyber Security in a better way. Now the question is what is Cyber law? "Cyber law is a generic term, which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyber law[2]."

[1] Author is a Student at K.L.E. Society's Law College, Bengaluru, India.
[2] PAVAN DUGGAL CYBER LAW 2ND EDITION

 [ISSN 2581-9453]

Why Cyber law is important? Cyber law is important because it covers and touches almost every aspect of transactions and activities concerning the Internet, Cyberspace and the World Wide Web. Now we have to know about what is Cyber Security. Cyber Security is the Activity which protects the information and information systems such as networks, computers, data, data base, data centres and applications with some procedure and technological security measures. There are many safeguards that protect data in our computer system such as Firewalls, antivirus software and other technological solutions for protection of computer and data in it. But it's not sufficient to ensure security. It's important for us to educate the people about the Cyber - Ethics, Cyber - Safety, and Cyber - Security related issues and these issues also need to be integrated into our Educational System as soon as possible so that people may know about any fraud or crimes happen to them and they will be aware of it.

Security is a measure which helps in ensuring confidentiality and integrity of information system from preventing any type of loss; it may be assets losses from Cyber Security attacks. There have been many recent changes in Cyber Security for computer systems and infrastructure. The main aim for the changes is to focus on protection of any kind of valuable information stored in any of the computer systems for adversaries who try to obtain , corrupt, damage, or are prohibited to access to it.

What is Cyber Security in legal Sense? According to **SECTION 2(1)(nb)** of The Information Technology Act 2000[3] - " Cyber Security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use disclosure, disruption, modification or destruction". In simple terms cyber security conjectures in one's mind, the image of security relating to computers in cyber space and security of procedures that happen in cyber space and the Internet. But if we see this definition we can say that, under section 2(1) (nb) the definition is given in wider terms. As it also deals with protecting information, equipment, devices, computer, computer resource, communication device and knowledge stored therein from unauthorised access. Therefore we can say that cyber security is concerned with the protection and preservation of the following[4] -

1. Information
2. Equipment

[3] PAVAN DUGGAL CYBER LAW 2ND EDITION (PAGE NO. 28 -29)
[4] PAVAN DUGGAL CYBER LAW 2ND EDITION (PAGE NO. 29)

3. Devices
4. Computer
5. Computer resource
6. Communication device and
7. All the information shared therein

These all should be protected from the following activities -

1. Unauthorised Access
2. Unauthorised use
3. Unauthorised disclosure
4. Unauthorised disruption
5. Unauthorised modification, or
6. Unauthorised destruction

Therefore we can say that the definition of "cyber security" under section 2(1) (nb) is given in wider terms. This section was drafted by lawmakers in futuristic terms, and they have kept in mind the developments that are going to take place in future.

According to **NATIONAL CRIMES RECORD BUREAU[5],** cyber crimes in India have gone up to 60% in the year 2012, approximately there were 3300 cases and in the year 2013 there were approximately 2050 cases reported in India. If we see some of the individual states in which more cases were reported in India according to NCRB, in Maharashtra 512 cases were reported, in Karnataka 400 cases and in Andhra Pradesh 450 were reported regarding cyber crimes in the year 2012. If we compare Cyber crimes with other crimes we can say that not a lot of investment is required as it can happen in several locations spontaneously. These crimes include Child pornography, counter fitting economic crimes, sexual exploitation, human trafficking, frauds etc.

There are five main reasons which give rise to cyber crimes-

- Nowadays more transactions are being online; therefore more data is also stored online. Other market information is also easily available. Therefore targeting online is very attractive and easy.

[5] https://ncrb.gov.in/

- As technology keeps on advancing day by day, many people use mobile phones for their easy connectivity. Due to this increase in latest threats keep on increasing. Hackers are also so advanced that they can easily crack the securities and get into the systems very easily.
- Many software's like virus and spy-ware are very much advanced and strong enough to take control on main applications and do not allow hackers to hack the main systems.
- If we talk about businessmen and vendors they are joined to systems to increase their profits. There are many E-Websites which are attacked on daily basis by dozens of hackers. They try to hack the system of website to shut down payment services and other services to other websites.
- As increase in technology made hackers also increase in their works and the software's which protects the system are not increased yet. The device that is used by hackers is Malware. This device is very much difficult to trace and they easily steal data for their gains.

Therefore we can say that the Technology is increasing or advancing day by day but, on the other hand the technology of Hackers is also advancing and they find loopholes in several systems to hack. To deal with this, the systems should also be upgraded continuously.

II. CYBER SECURITY

We have already seen the meaning of Cyber Security, but before we start it in detail we will see the meaning of Cyber Security again. According to **SECTION 2 (1)(nb)** of the Information Technology Act 2000 it states that[6] - " Cyber Security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use disclosure, disruption, modification or destruction". In simple words we can say that it is a collection of tools, policies, security safeguards, guidelines, assurance and technologies that is or can be used to protect the Cyber environment, organizations and user's assets. What are the things included in Organizations and User's Assets is infrastructure, applications, services, telecommunication services and systems and the stored information in the Cyber Environment.

Now we will be seeing that how Cyber Security has been evolved in world and in our

[6] PAVAN DUGGAL CYBER LAW 2ND EDITION (PAGE NO. 28)

country. Evolution[7] -

- **VIRUSES (1990s) - ANTI-VIRUS, FIREWALLS**
- **WORMS (2000s) - INTRUSION DETECTION AND PREVENTION**
- **BOTNETS (LATE 2000s TO CURRENT) - DLP, APPLICATION-AWARE FIREWALLS, SIM**
- **APT, INSIDERS (CURRENT) - NETWORK FLOW ANALYSIS**

So we can say that the latest Cyber Security we are having right now is APT, INSIDERS which is Network Flow Analysis.

Cyber Security ensures the safety and maintenance of the security properties of the Organizations and User's Assets, Cyber Security protects them from risks in networked environments. Cyber Security is bodies of Technologies which is designed to protect network, computer systems, programs and data from several attacks and from unauthorised access. Elements which are included in Cyber Security for the protection of systems are -

1. Many application securities which are used for software, hardware and several other methods which are used to protect application from external threats.
2. Information security is one of the best element which is used to avoid information from unauthorised access, disclosure, disruption and from recording or destruction. Information Technology Security and Information assurance are two major elements and aspects of Information security.
3. Securities which are adopted by Network Administrators consist of several provisions and policies. These provisions and policies prevent unauthorised access, misuse or modification of computer and computer network. Network Security involves the authentication to access the use of data which is controlled by Network Administrators. Users who use them are given their personal ID and passwords for using it. Network Security covers many varieties of computer networks which include both public and private networks. As they are used for many purposes like making transactions, communication between governmental employees, businessman's and many individuals.
4. Data Recovery and Business Continuity planning which is also known as DR/BC plan. This majorly focuses on systems recovery[8].

[7] https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
[8]https://www.undp.org/content/dam/albania/docs/STAR/Disaster%20Recovery%20and%20Bussines%20Continuity%20Plan.pdf

5. The Educations of End-users is also important as they should also know about several attacks and how to avoid them. We should provide them with suitable education about what are the precautions and remedies to avoid cyber crimes[9].

So, these are some of the elements which are given under Cyber Security. In this we have also seen that End-users should also give suitable education relating to cyber crimes and how to avoid these crimes. And if by mistake they are victims of any cyber crime proper action should also be taken against them.

III. INDIAN SITUATION

Under this topic we will be seeing the Indian Cyber Situation and comparison with some other countries[10].

- India is considered to be at 3rd rank in terms of highest number of internet user's in the world after United States of America and China. According to reports by some authorities the internet number usage in the country has grown 6-fold between 2012-2017 and compound annual growth rate is 44%.
- India is considered to be at top amongst the top 10 spam sending countries in the whole world alongside with United States of America.
- India is ranked under top five countries in the world which is affected by Cybercrime. According to a 22 October report by an online security firm "Symantec Corp".

IV. CYBERATTACKS IN INDIA

There are many Cyber attacks in India everyday and every time. Government of India has also taken some initiatives after seeing increase in Cyber attacks cases. Some of the main cyber attacks cases are[11] -

JULY 2016 - UNION BANK OF INDIA HEIST - In this case the hacker had sent an email to an employee working in Union Bank. Through that the hacker had taken all the information and he accessed the credentials to execute a fund transfer of $171 millions, but the action was taken very quickly by the bank which helped the bank to recover almost entire money.

MAY 2016 - WANNACRY RANSOMWARE - In this case, the global ransom ware attack

[9] https://www.cyberdefensemagazine.com/end-user-security-education/

[10] https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
[11] https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

took its tool in India. Due to this several thousands of the computers were locked down by ransom-seeking hackers. This attack also had its impact on Andhra Pradesh police and state utilities of West Bengal.

MAY 2017 - DATA THEFT AT ZOMATO - In this case, the food tech company name " ZOMATO " , discovered that data including name, email ids and passwords of 17 million users were stolen by an " ethical " hacker who later demanded that the company should acknowledge its security and later the hacker had put up for sale on the Dark Web.

JUNE 2017 - PETYA RANSOMWARE - In this case, the ransom ware attack made its impact around the world and this impact was also seen in India, where container handling functions at a terminal were operated by DANISH firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port trust which got affected.

These were some of the latest Cyber attacks that were faced in India. Although at the correct time these were stooped and situation was normal again in the Country.

V. CHALLENGES IN INDIA FOR CYBER SECURITY

Cyber Security is or has been considered to be one of the most challenging securities in India and it is also considered as national security problem. In a report it was mentioned that the Government of India had made a notice that Cyber Security must and will be the top priority for the country, but nothing like this happened. Some of the challenges that are faced by India are[12] -

- **LACK OF UNIFORMITY IN DEVICES USED FOR INTERNET ACCESS -** India is a country where people mainly belong to middle class families and are not so rich, therefore it is not possible for everyone in our country to buy expensive phones. We know that in United States of America Apple (mobile company) has 44% of market share. In India the I Phones with good security or higher security are used by only 1% in our country. Therefore there is a very much big gap between the high-end phones and lower costs mobiles which makes impossible for legal and technical standards to be set for data protection.
- **LACK OF NATIONAL LEVEL ARCHITECTURE FOR CYBERSECURITY -** There is no such good national security architecture that can fulfil the efforts of all the agencies that can protect us from cyber crime and can build a good security system.

[12] https://analyticstraining.com/cyber-security-challenges-in-india/

The Prime Minister's office has created a position towards this cause, but it's not that satisfying. Although India has a necessary structure in place.

- **LACK OF SEPARATION -** If we compare India with other countries and states, in cyberspace there are not such any types of boundaries. Therefore for making the digital assets of ONGC, banking functions etc. which can be exposed to the possibility of Cyber attacks from anywhere. But this could result in security breaches at a national level, and loss of money, property and lives will be more. Therefore to tackle this situation we need technically equipped multi-agency organization that can create a very good and sound strategy for tackling these issues.
- **LACK OF AWARENESS -** There is no such National Regulatory Policy in India for cyber security at both company level and individual level. Individuals can be protected from Cyber attacks only if they are guided and supervised by legal framework.

As we know that India has one of the best Information Technology and highly skilled workforce, therefore efforts can be made towards strategic use by the Government. The incentives provided by the Government can encourage private sectors towards creating a new agency that will focus on National Cyber Security. Therefore with strong cyber security defences Indian's can create a safe and better Digital India.

Now the big and major part is that how a hacker can attack on our Computer systems or any other systems and through which tools hacker can hack our systems that we use in daily lives. Therefore now we will see the methods of attack -

Methods of Attack:

The most commonly used weapon by any hacker to hack into our computer system is through viruses and worms. These types of attacks can be classified into three types of categories, these are -

1. **Physical Attack -** In this the infrastructure of the computer is destroyed by bombs, fire etc.
2. **Syntactic Attack -** In these types of attacks mainly viruses are used to damage computer infrastructure. Due to this the computer also gets slow and it becomes unpredictable.
3. **Semantic Attack -** In these types of attacks all the information that are kept in the system is fully destroyed without the knowledge of the user.

So, these are the three kinds of Attacks that can be done by the Hacker in our computer

system. Therefore now the question is, if we are being attacked or before being attacked how can we protect our system or how can we avoid such attacks to enter into our system. Some of the measures to avoid these attacks are -

The first step to protect your self is to recognize the risks and we should become familiar with some of the terminologies associated with them -

- **VIRUSES -** This type of strong and malicious code can be there in your computer system, it can come through downloading any stuff from any unknown sites or any sites which are not safe. These can also come into our computer systems while opening email and downloading attachments.
- **WORMS -** This is also a type of Virus and they can enter into computer systems with the knowledge of the user. When they enter into any system they start to damage the system from its core that is the motherboard of the system, and once they start damaging the worm will attempt to find and infect the other computer systems. Worms can also enter through email, or by any web sites and infect our software.
- **TROJAN HORSES -** This is a very strong type of virus and it does not infect our computer system but it actually finds confidential information from our system and transmits them to hackers or intruders.
- **HACKERS -** These are the ones who exploit weakness into our computer system and software for their personal gains. This is illegal and its violation of our right of privacy and it attracts many other penal provisions and Constitutional Provisions. Their main intention is only to get our personal information from our computer system for anyone.
- **EMAIL CRIMES -** We get many spam messages on our email ids and these messages are used to infect our system by virus and worms. These e-mails contain viruses and worms and as we open them they start infecting our system and transfer our information to the hacker or any intruder.

So, through this we can see that we should never open any website in our computer system that can insert viruses and worms. And if our computer system is hacked we should report to Cyber police stations as our information can be misused by the Hackers.

VI. NEED FOR CYBER SECURITY IN INDIA

Approximately 8% of the houses in India are having laptops or Desktops. Three Union Territories in India namely Chandigarh, Delhi and Goa have the highest number of computer

usage.

According to reports taken in 2011 census, approximately only 3.0% of the total houses in India have internet connectivity. The census covered 245 million houses in India and from these only 3.0% peoples are having internet connectivity. Internet includes both Broadband connections and low speed connections. If we see the reports of Internet World Stats on June 30 2012, there were 2.3 billion internet users worldwide and China was the biggest user. Over 530 million users were from china.

It's very important for India to develop a good and strong Cyber Security. Information is one of the most valuable asset for any individual, cooperate sector, state and country with respect to an individual. Some of the concerned areas are -

1. Protection from unauthorised access, disclosure, modification of the resources of the system.
2. As technology is increasing so security should also be developed when an individual is making any online transaction regarding shopping, banking, railway reservations and other things.
3. There are many social networking sites nowadays in which our personal data and information is stored. Therefore security regarding Hijacking of accounts should be seen.
4. One of the most important things for improving Cyber Security is that we should have a better understanding of the threat and of the weapons used by the attacker to make better cyber defences.
5. Every unit of cyber security should handle different kinds of units and not only one.
6. Not all the organizations face same attacks, therefore every organization should prepare themselves well to deal with the attack and cyber security should be good.

These were some of the areas where India needs to develop its cyber security very strong and well and should be well prepared to deal with any kind of cyber attacks.

The above points dealt with banking sectors, social networking sites, co-operate sectors and online transactions. Now we will see what changes we need in Educational System to create Awareness about Cyber Security. Some of the elements are -

In Education Students

- Must be aware of possible attacks and types of intruders.

- They must also be aware of some legal terminologies such as VIRUS, TROJAN HORSES and WORMS
- Other terms like SOFTWARE/HARDWARE, DESKTOP SECURITY, WIFI SECURITY,
- How to secure Password, attacks relating to Social Networking sites and malicious software like:
    - Phishing, Hoaxes
    - Scare ware, Malware, Virus ,Worms
    - Trojans, Botnet, Sypware

In schools the students only gets knowledge about information technology skills. This marks question on the teachers and the educational system to ensure that positive habits of on-line behaviour are being formed. On the other hand we see teachers in the schools don't have such good information about cyber security and lacks the knowledge about it, and they are not up to date with information related to cyber awareness issues, especially with respect to securities. Therefore teachers should be given special training for that.

VII. LEGAL FRAMEWORK FOR CYBER SECURITY IN INDIA

There are some of the laws and acts which deal with cyber attackers and cyber security in India. These are -

- **INFORMATION TECHNOLOGY ACT 2000 -** Under this, Section 43, 65 and 66 are used to give punishments to the attackers or intruders.

SECTION 43 - Penalty and compensation for damage to computer, computer system, etc[13].

SECTION 65 - Tampering with Computer Source Documents[14].

SECTION 66 - Computer-Related Offences[15].

- **INDIAN COPYRIGHT ACT -** This act clearly states that if anybody or any person knowingly makes use of an illegal copy of computer program shall be punished. Computer programs have copyright protection but they don't have patent protection.
- **INDIAN PENAL CODE -** Under IPC Section 406 and 420 are used to give punishments to the attackers or intruders.

[13] PAVAN DUGGAL CYBER LAW 2ND EDITION (PAGE NO. 115)
[14] PAVAN DUGGAL CYBER LAW 2ND EDITION (PAGE NO. 202)
[15] PAVAN DUGGAL CYBER LAW 2ND EDITION (PAGE NO. 205)

SECTION 406 - Punishment for Criminal Breach of Trust[16].

SECTION 420 - Cheating and dishonesty including delivery of Property[17].

- **INDIAN CONTRACT ACT -** This Act offers remedies in case of breach of contract, Damages and Specific Relief performance of the Contract

These are some of the laws and acts which deal with cyber security in India and gives the Punishment to the offenders, attackers or intruders.

VIII. CYBER SECURITY INITIATIVES TAKEN BY THE GOVERNMENT

In today's world the threats associated with technology is not just for business but also for Governmental Authorities. There are many initiatives taken by the Government of India to deal with the threats and those initiatives are in the right move to create and maintain a secure cyber environment. Following are the major initiatives taken by the Government of India[18] -

1. **INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-In) -** This is a national nodal agency for the emergency response of any kind of cyber securities breaches or attacks. Departments have been directed to directly inform CERT- In for any kind of cyber security breach. This also issues guidelines to tackle the risk. In September 2019 CERT-In informed about NECURS MALWARE.
2. **NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE (NCIIPC) -** National Critical Information Infrastructure Protection Centre was founded in 2014. The main aim and objective for this was to minimize the risks. NCIIPC organization is created under Section 70A of The Indian Information Technology Act 2000.
3. **GUIDELINES FOR ORGANIZATIONS CISOs. –** These guild lines are issued by Ministry of Electronics and Information technology. These guidelines are issued to chief security officers to make sure that they are following best cyber security practices.
4. **CYBER SWACHHTA KENDRA (BOTNET CLEANING AND MALWARE ANALYSIS CENTER) -** Government of India under Ministry of Electronics and Information Technology launched Cyber Swachhta Kendra to maintain strong cyber security and safe cyber environment. It works for both mobiles and computer devices.

[16] UNIVERSAL'S CRIMINAL MANUAL 2016 (PAGE NO. 565)
[17] UNIVERSAL'S CRMINAL MANUAL 2016 (PAGE NO. 569)
[18]https://www.cxovoice.com/cyber-security-initiatives-by-government-of-india-to-combat-cyber-threats/

5. **REGULAR AUDIT OF GOVERNMENT WEBSITES -** For the safety of devices and systems Ministry of Electronics and Information Technology has asked to audit all the websites before uploading into main server to make sure that there are no hidden viruses in it.
6. **CRISIS MANAGEMENT PLAN -** To face all kinds of cyber threats Government of India has formed CRISIS MANAGEMENT PALN. This plan will only implement in critical sectors.
7. **REGULAR TRAINING PROGRAMS -** As technology is increasing day by day, so the attackers' weapons are also changing with technology, therefore, to keep pace with them the Government of India has announced to conduct regular Training programs for CISOs and network and system administrators.
8. **PERSONAL DATA PROTECTION BILL -** This bill was introduced in the year 2019 to store all the personal data in India only, nobody can possess it abroad without the permission and approval of DATA PROTECTION AGENCY. This bill was introduced as many mobile apps and websites take permission to store our information on their server.

These are some of the major initiatives taken by the Government of India for Cyber Security. And these are one of the best initiatives taken by the Government of India.

IX. EDUCATIONAL INITIATIVES ON CYBER SECURITY TAKEN BY GOVERNMENT

As we have seen earlier that students in schools are not taught about the cyber attacks and cyber securities. Neither teachers are aware nor are they up to date with cyber securities and attacks. Therefore here are some of the initiatives taken by the Government of India in Educational Sectors[19] -

- **INFORMATION SECURITY AWARENESS -** This initiative is launched every five years of period. The objective and main aim to launch this initiative is to create awareness about Information Security to students and children even to non IT professionals in a very good and systematic manner.
- **INFORMATION SECURITY EDUCATION AND AWARENESS PROJECT -** The main aim and object of this initiative is to train system administrators by offering many Diploma Courses in Information Security, and some certificate courses in Information Security. This is also for all Governmental employees and officers to get

[19] https://niccs.us-cert.gov/

them trained. Through this everyone will be getting to know about cyber securities and various cyber threats they are surrounded with.

- **NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) -** The main objective and aim to make this is to continually improve cyber security educational programs for the country, to use a strong and sound cyber practices that will make more strong security for the country.

X. CONCLUSION

The Government of India has done and given much support for cyber security as we have seen, by taking so many initiatives and all the initiatives are very good. As technology is changing day by day and keeps on improving so the major threat to all of us is cyber attack and to deal with this we need to develop new cyber securities from time to time. Cyber awareness and computer hygiene should become an integral part of our lives as the digital education has become. With every new invention there comes a change in society and the way we deal with it. To deal with these we all need to come together and make a new and a better Digital India for our upcoming generations and we should also try that the threats we are facing today will not be faced by them in near future. It's everyone's responsibility to let no one be tricked by the hackers out there and start from your family. Parents should be aware about the social media life of children and make healthy and friendly relation with them so that they share everything. Change in thinking, strategy and maturity is essential for cyber security in today's world of digitalisation. And off course the cyber security management team needs to level up the game with the hackers every now and then to prevent cyber attacks. Cyber security needs to be dealt with in a responsible manner.

*****