# World of Cyber Space: Cyber (Crime, Security, Law) and Cyber Solution

– Vishal Kumar
Security Architect, OYO Rooms, vishalthakur88@gmail.com

The Cyber world is governed by the use of mobile, computer, electronics and electromagnetic spectrum to store, modify, and exchanged data via networked systems and associated physical infrastructures. The Cyber world can be seen as the space in which computer transactions occur, specifically transactions between different computers, different networks, data, databases, images records, personal information and text on the Internet exist in cyberworld. It is global spectrum within the information environment consists of the interdependent network of information technology infrastructure, including the computer systems, mobile networks Internet, telecommunications networks, and IOT.

## Introduction

In this present era, cyber space domain provide reliability & flexibility leading to its use with the government framed internet norms, Internet along with making life easier with economy activities like purchasing, selling, online transactions and social networking brings along many cyber threats. The internet has simplified business processes such as editing, summarizing, coding and sorting. Cybersecurity refers to a global and dynamic spectrum characterized by the combined use of electronics and electromagnetic domain, whose use is to modify, exchange, share,create, store, and extract, use, eliminate, inform and break physical resources.

**Cyber crime** is a sequence of organized crime attacking network and cyber security domain. Cyber crime such as hacking into Web Application, Computers and personal & payment information.A crucial impact from cybercrime is financial concern and cybercrime can include many different

domains of profit-driven criminal activities including email & internet fraud, identity fraud andransomware attacks as well as attempts to steal financial accounts, credit card or other payment card information. There attack vector can be through a network system & clicking into unreliable links connecting to unauthentic Wi-Fi, downloading software and files from unsecure sites, power consumption, electromagnetic waves and many other spectrum.

However, Cyber security is a severe issue and should be taken into considerationimmediately because it has arised to become a national level concern. Presently, most electronic appliances such as Computers, laptops and cell-phone have by default in-built firewall security software but despite of this the Computation isn't 100 percent accurate & reliable to protect our data. Cyber security consists of processes,technologiesand controls designed to safeguard systems, networks and data from cyber threats. Effective cyber security reduces the risk of cyber attacks and protects against the unauthorized exploitation of networks, computer system and technologies.A Well-defined cyber security domain involves implementing controls based on three spectrums: people, processes and technology. This three-pronged methods helps organizations safeguard themselves from both organized attacks and common internal attack such as accidental breaches and human errors.Computers can be protected through well designed software and hardware.

## II. Overview of Cyber World Space, Cyber Crime and Cybersecurity

The information technology sector is becoming increasingly integrated with physical infrastructure & operations. There is subsequent risk for wide scale that could cause harm or disrupt services upon which our economy and daily lives of millions of Internet User's depends andthe network which is interdependent of information technology components that undermines many of our communications technologies inaccordance today. Cyber space is an electronic medium used to form a global computer network to facilitate online communication. It is a huge networking of computers made up of several worldwide computer networks that employs various protocols to take in communication and data exchange activities.

Crimes are now being executed through cyberspace domain largely. This includes the conspiracies, banking and financial fraud,production and distribution of pornography & child exploitation intellectual Property violations and other crimes, all of which are subsequently human and economic impacts. Country's economic vitality and national security depend on a vast array of critical network systems, services, and resources known as cyberspace. Cybersecurity has changed the ways we power our homes, run our economy communicate, travel and obtains government services.


Cyber crime defines the subsequent & organized way of crime affecting both cyber space and cyber security. Cyber crime refers to criminal activity done using computers and the Internet. It also involves illegal access (unauthorized access, transmissions of computer data, to, from or within a computer system .This conveys anything from downloading illegal files to stealing millions of dollars from online bank accounts. Cybercrime also consists of non-monetary offenses such as distribution & creation viruses on other systems are highlighting confidential business information on the Internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the internet to steal personal information from other users.

Cyber-security is a broad spectrum of technology, processes and practices designed to safeguard networks, computer systems, programs and data from threats, damage, or authorized access. In the computing or cyber context, the word security simply implies Cyber-security. Ensuring cyber-security requires coordinated efforts from both the citizens of the India and their information system. The adverse effect posed by breaches in our cyber-security is increasingly fastly than we can keep up with it. It is difficult to concentrate efforts on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. This makes us to lead that we have to attack cyber security breaches as a whole. Cyber security is the combination of safeguards, guidelines, risk management approaches, tools, policies, security concepts, security actions, training, best practices, assurance and technologies that can be used to protect the cyber space and organization and user□s confidential information.

Organization and user□s assets include web applications, services, telecommunications, computing devices,personnel,infrastructure,,and the totality of transmitted and/or stored information in the cyber environment. Cyber security thrives to ensure the

conspiracy and maintenance of the security properties of the organization and user's confidential assets against relevant security risks in the cyber environment. Cyber-security is a broad domain of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risk. Most cyber criminals and nation-states among others, present risks to our economy and national-level security. Cyber-security is a texture of technology, processes and practices designed to protect computer system, programs networks, and data from attacks, damage, or authorized access.

**A. Importance of Cyber Security**

The following are the importance of cyber security:

- To work collaboratively with public, private and international entities to secure cyber space.
- To help individuals and institutions develop and nurture a culture of Cyber security. which may include Confidentiality, Integrity & Authenticity.
- To help understand the current trends in IT/ Cybercrime and develop effective solutions.
- To help people reduce the vulnerability of their information.

**B. Types of Cyber Frauds**

There are multiple cyber crimes, but this paper will examine the cyber crimes that are dominating India based on current trends;

- **CXO Email Scam:** It is a phishing scheme that attempt to obtain sensitive information such as usernames, passwords and creditcard details by disguising oneself as a trustworthy entity in an electronic communication..The cyber criminals achieve this by researching employees who are in charge of finance and request a fraud transfer to fraudulent account claiming to be CXO.

- **Cyber Terrorism:** It involves the use of internet space tocommit terrorism or procure terrorist attacks. This is a new means which insurgents or religious extremists use to recruit new members and form strategies on how to attack nations.


- Ransomware: With the rise of ransomware as- service, cybercriminals can now purchase a user friendly kit they could deploy with little or no cyber expertise from the dark web. A Ransom ware is a type of malware that infects a machine when user clicks on a seemingly legitimate link and unknowing downloads a malicious file. The virus will then encrypt the user's files, share devices and servers. Leaving them inaccessible unless the victim pays for the decryption key usually in cryptocurrency.


- **Fraud- Identity Theft**: It is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name,[1][2]and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences,[3] especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The concept is simple; someone gains access to your personal information and uses it for it for his own benefit .

- **Internet Pornography**: The use of the web for sexual abuseremains a very active research interest. It has been found that internet pornography is a disturbing trend especially among the youths. It also involves using internet to download and transmit pornography pictures, photos, writings etc. Internet is used as an avenue for luring unsuspecting children to pedophiles, and for distributing child pornography. Another trend is the use of mobile phones and internet for prostitution.

Hence, prostitutes now advertise their trade via internet by exposing their sensitive, sensual and private parts to the internet users.

- Cyber Plagiarism: It is not in itself a crime, but like counterfeit can be punished in a court for prejudices caused by copyright infringement, violation of moral rights, or torts. In academia and industry, it is a serious ethical offense.Plagiarism andcopyrightinfringementoverlap to a considerable extent, but they are not equivalent concepts, and many types of plagiarism do not constitute copyright infringement, which is defined by copyright law and may be adjudicated by courts.

- Hacking: Hackersis any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software.

Hackers can also track what one will do on their computer and can also import files on our computer. A hacker can install variousprograms on to your system without your knowledge. Such programs can also be used to steal personal details such as passwords and credit card information. Crucial data of an organization can also be hacked to get the secret details of the future plans of the company.

## III. CAUSES AND EFFECT OF CYBER CRIME IN INDIA

Cyber crime is increasing astronomically and some of the causes (reasons) for the vast increase of internet fraud in world are:

- **Greed and Easy way :** Most people actually involve in cyber crimes not becausethey don't have what it takes to live a normal life but because they are never contented with what they have and the desire to have quick and more wealth without having to go through the legitimate manner.

- **Lack of Confidence:** It is one of the reasons people engage intocyber crimes. Some people believe they can no longer make it in life, they feel disappointed and they think the only way to make up their mistakes and to move forward is by making quick wealth, In this case they fall back to internet fraud.

- **Unemployment:** This is one of the major reasons people getinvolved in cyber crimes. After all educational qualifications one seems to have obtained, jobs are still not available for them and this lead to frustration and for them to live an average life, they see internet fraud has a means of survival. Even the employed are not paid for months, sometimes years and this can also lead to individuals engaging in Cyber crimes.

Resident's activities impact to Digital India.

Lag in Cyber Security Awareness.

SlowInternet connectivity & lack of govt offered security tools.

Lag in Good Initiatives towards Cyber Security.

### A. EFFECT OF CYBER CRIME

- **Reduces the Competitive Edge of Organizations:** Computer crimes over the years have cost a lot to individuals, private and public business organization in India, causing a lot of financial and physical damage. Due to cyber crime, there has being loss of billions, such crimes may threaten a nation's security and financial health.Cyber crimes has immense impact towards India economy e.g the recent ponzi scheme such as Crypto Ponzi Schemes etc in which many Indians were engaged. It has been encountered that Indians lost millions this scheme which is a huge loss to Indian economy and its concerned people.

- **Time Wastage and Slows Financial Growth:** Time Wastage is another concern because many IT personals may spend a lot of time on handling harmful incidents which may be caused by cyber criminals. The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enter in an organization

and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contains confidential information like credit cards of clients and as the data are stolen the client will not have faith towards the company again and will move to someone else who could safeguard their confidential details.

- **Slows Productivity and Add to Over Head Cost:** Cyber crime impacts the productivity of a company, as an organization will take measure to reduce cybercrime, by entering more password or some attempts this will take time to do and therefore will affect productivity. Cyber crime will imapct the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks.

- **Defamation Of Image:** With increase in cyber crime activities in our nation is an undesirable movement towards the nation growth. When people's involved are caught, it exempts the image of the family of that people. Other effects includes the consumption of computer and network, can also cost an individual involved his education and career when caught and it deprives him of becoming who he wants to be in life.

## B. COMBATING CYBER CRIME

The postulates below are very crucial in combating cyber crime activities:

- **Use of legislation:** This is a very crucial step towardsde-aligning cyber crime. The government both state, local and central should have proper legislation that will stipulate adequate punishment for these cyber frauds. The issue is that most countries laws aren't strong which allows these cyber frauds to hit from international borders and remain untracked. Even when caught these criminals avoid being extradited to a country, such as the US and Europe, that has developed laws for prosecution. GDPR is an example from European union. The IT Act 2000 India attempts to change outdated laws and provides measures to deal with cyber crimes. We require such laws so that people can perform transactions over the internet through credit cards without any sort of fear. The Act provides the legal framework so that data is not denied legal effect, or validity, solely on the ground that it is in the electronic records.


The **General Data Protection Regulation** ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

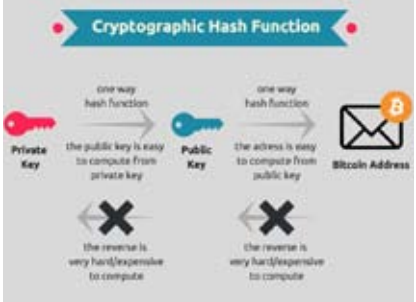
- **Creation of awareness:** As technology is advancing so more people rely on the Internet to store sensitive data's such as banking/credit card information, criminals are trying to steal that information. Cyber crime is becoming critical threat to people across the globe. There must be an awareness about how information is safeguarded and the tactics criminals use to steal data. The government as an urgent need should make sure that the people are aware about the activities of these hoodlums and how to safeguard their files, systems, networks etc from unauthorized access. Also, the NGOs (Non-governmental organisations) and anti-crime agencies should make sure that, this trend is reduced to the barest minimum if not eradicated fully.

- **Use of Cryptography:** Cryptography is an important aspect when we deal with network security. 'Crypto' means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. These both terms are a subset of what is called as Cryptology. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption).

Individuals who practice this field are known as cryptographers.

- **Confidentiality:** Confidentiality is a security aspect which ensures that the data of the user is confidential and isn't accessed by any unauthorized party/ individual.

- **Integrity**: Integrity ensures that the data received is exactly as sent by an authorized entity The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information. Authentication: The sender and receiver can confirm each other's identity and the origin/destination of the information.




## IV. MODELS OF CYBER SOLUTION

Legislature should enforce strict laws, providing penalties for any individuals involved in any sort of cybercrime in India. This will arise fear in the people because of the punishment involved. I also believe that there should be more agencies in charge of cybercrime,cyber crime working group. Since poverty is one of the major reason behind internet fraud in world, government should encourage poverty alleviation programmes in order to reduce the rate of poverty in India. Also, free education should be encouraged by the government to enable those who can't afford the fees paid in private schools.

Cybercrime in any country is tough to prove as it lag behind the traditional paper audit trail, which requires the expertise of specialists in computer technology and internet protocols hence data should be stored within country and we need to create awareness to companies and citizens that if they are going to use the internet,need to provide services, they should maintain data localization and update the security on their system. There's also great need to educate both Public & Private sector organizations for effective security management. We need to thrive data storing (localization of data) with in country.

The organizations are now adopting a policy that all systems in their purview must meet strict security guidelines. Automated security updates are sent to all computers and servers on the internal network, and no new system is allowed online until it confirms to the security policy.


Next Gen Firewall, EDR, IPS/IDS and Anti Malware protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall/IPS/IDS typically guards an internal computer network against malicious access from outside the network. Agencies undertaking to safeguard against cyber crimes should be equipped and should have proper knowledge of the internet to know from the issue is arising and how to deal with them.

Lastly, Youths should be empowered with different skills such as tailoring, hairdressing, shoe making etc in order to be financially strong and this will reduce the rate at which cyber crimes is evolving. Since the level of unemployment in the country has increased significantly towards e-crime in India, the government should create employments for these youngsters and set up IT laboratories/ forum where these youths could come together and highlight their Knowledge/Interpersonal Skill. This can be used synchroniously towards developing IT in India as well as they can be rewarded handsomely for such good deeds.

## Conclusion And Future Work

Information and Communication Technology (ICT) systems has evolved immensely in India. Many corporate organizations and public sector firm depend on ICT and computer networks to perform simple as well as complex jobs. However, the cyber space is immensely becoming vulnerable as many businesses, agencies and individuals are being swindled by cyber criminals in the country.

Cyber crime is rising at an alarming rate in our country. Our country is ranked third in global internet crime after the United States of America

and United Kingdom while 7.5 percent of the world's hackers are said to be Indians. Committed mostly by the youngsters, often called "yahoo" boys, the fraudsters are increasingly taking benefit of the rise in online transactions, electronic shopping and e-commerce to indulge in cyber crime. Thus, cyber security must be taken as a crucial concern as it is affecting the image of the our country globally.

- Cyber Education is a crucial weapon for Cyber literacy, as such seminars and workshopsshould be organized periodically with emphasis on cyber safety so that individual will learn to keep their personal data's safe and youth will flee cyber crime.
- Government should take appropriate measures for intensive training of law enforcement agencies on Cyber Security so that they can track down the cyber criminals, no matter how much excel in this field.
- Financial institutions in India should encourage development of fraud detection departments. There should be a centralized electronic data bank containing specific Information on each individual resident and visitor to India.
- We must highlight some eGov initiatives like Cyber Surakshit Bharat, Cyber Saksharta Abhiyaan, Cyber Swacchta Kendra etc and the need to take them to masses.
- Role of Industry may also be added where in courses are being imparted by the OEMs to make the future generation cyber aware.
- Some periodic Seminars/ Workshops should be conducted to create awareness among the people about the Causes & Effects of Cyber Attacks and measures to be taken for mitigating such problems.

## References


- The Information Technology Act, 2000- Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000.
- "Section 66A of the Information Technology Act". Centre for Internet and Society (India). Retrieved 14 April 2015.
- Hunton, Paul. "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model." *Computer Law & Security Review* 25.6 (2009): 528-535. *Academic Search Premier*. EBSCO. Web. 22 Jan. 2011.
- Ghosh, Sumit. "The Nature of Cyber-attacks in the Future: A Position Paper." *Information Systems Security* 13.1 (2004): 18-33. *Academic Search Premier*. EBSCO. Web. 19 Jan. 2011.
- 145U.S. Department of Justice. National Institute of Justice Research Report. Electronic Crime Needs Assessment for State and Local Law Enforcement. National Institute of Justice, March 2001.
- Wall, David S. "Catching Cybercriminals: Policing the Internet." *International Review of Law, Computers & Technology* 12.2 (1998): 201-218. *Academic Search Premier*. EBSCO. Web. 19 Jan. 2011.
- Enterprise Survival Guide for Ransomware Attacks. Author: Shafqat Mehmood, shafqat.mehmood@me.com Advisor: Adam Kliarsky
- Justice, Bureau of Justice Assistance U.S. Department of. "Internet Crime Complaint Center." 2009 Internet Crime Report (2008).
- Official (ISC)2 Guide to the CISSP CBK ((ISC)2 Press) by Adam Gordon.
- CISSP (ISC)2 Certified Information Systems Security Professional Official Guide by James Michael Stewart, Mike Chapple and Darril Gibson.
- "The Information Technology (Amendment) Act, 2008". Retrieved 7 May 2017.


**Vishal Kumar** is a law graduate in cyber law and is a Certified Cyber Security Professional presently associated with OYOROOMS as a Cyber Security Architect.

vishalthakur88@gmail.com