UNDERSTANDING CYBER CRIME AND CYBER SECURITY MEASURES

By

—**KADEKA SAINANDA**, Asst. Professor,
Aurora's Legal Sciences Academy
Hyderabad
Email : parisainandachowdary@gmail.com

Unlike the crime in a physical scenario and its containment, cybercrimes are technological in its essence, anonymous in its operation and untraceable in its gateway. Everybody thinks that only stealing someone's private data is Cyber Crime. But in defining terms we can say that 'Cyber Crime refers to the use of an electronic device (computer, laptop, etc.) for stealing someone's data or trying to harm them using a computer. Besides, it is an illegal activity that involves a series of issues ranging from theft to using your system or IP address as a tool for committing a crime.

Introduction :

Cybercrime is the most discussed issue of the 21st century. The technology sector worldwide is witnessing a boom in the consumer of smartphones and the internet which is raising concerns with regard to the privacy and security of the users. Owing to this reason, it is highly essential for all the users to know about cybercrime & security.

Cybercrime is a dangerous attack on company or an individual or on Government Agencies. There are many cases where the cyber-attack has brought massive loss to the company and individuals due to the data hack. We live in a technology-driven era, and every piece of information is now fed on computers. Cybercrime involves an attack on computers and digital devices. These cyber-attacks can prove hazardous not just for the organization, but also for the nation. To date, there are many digital attack cases in India and global, pushing for more security measures. These attacks are also affecting the economy of the country if not controlled in the initial stage.

Cybercrime in the context of Internet :

Cybercrime or attack is defined as the systematic criminal activity occurring digitally and done by attackers. There are many examples of cybercrime, including fraud, malware viruses, cyber stalking to cyber terrorism and others. Due to these, government agencies and companies are investing more in the maintenance and hiring of cybercrime experts. In the initial period, cybercrime was committed only by individuals or by small groups. However, now a highly complex cybercriminals network work on attacking the system for data collection and it is great threat to the individual or company including government agencies.

In the current context, the countries following the western jurisprudence and common law systems have a well evolved criminal law and criminal justice administration to tackle the physical world of crimes. Such systems look at crime from the four elements of Mensrea, Actus Reus, and Criminal Act and forbidden by Law and in the criminal act in the physical world is dealt on the above basics.

The Cyber world is defined as a virtual world which is different from that of the physical world. The cyber world though a virtual world is a reality, which interconnects people, organizations, Governments etc., It transacts information at the basic level but also conduct the business of governments

and private in a manner where no other technology could dream of.

Cyber Warfare:

Snowden revelations have shown that Cyberspace could become the theatre of warfare in the 21st century. Future wars will not be like traditional wars which are fought on land, water or air. When any state initiates the use of internet-based invisible force as an instrument of state policy to fight against another nation, it is called cyber war.

It includes hacking of vital information, important webpages, strategic controls, and intelligence. In December 2014 the cyber-attack a six-month-long cyber-attack on the German Parliament for which the Sofacy Group is suspected. Another example 2008 cyber-attack on US Military computers. Since these cyber-attacks, the issue of cyber warfare has assumed urgency in the global view to safeguard the interest of individuals, companies and Government agencies.

Types of Cyber Crimes :

Speaking in a broadway we can say that Cyber Crime are categorized into four major types. These are Financial, Privacy, Hacking, and Cyber Terrorism.

The financial crime they steal the money of user or account holders. Likewise, they also stole data of companies which can lead to financial crimes. Also, transactions are heavily risked because of them. Every year hackers stole lakhs and crores of rupees of businessmen and government. Privacy crime includes stealing your private data which you do not want to share with the world. Moreover, due to it, the people suffer a lot and some even commit suicide because of their data's misuse. In, hacking they intentional deface a website to cause damage or loss to the public or owner. Apart from that, they destroy or make changes in the existing websites to diminish its value.

Modern-day terrorism has grown way beyond what it was 10-20 years ago. But cyber terrorism is not just related to terrorists or terrorist organizations. But to threat some person or property to the level of creating fear is also Cyber Terrorism to the entire world.

And further to deal with the cybercrimes, which may not have found a definition under the Indian Penal Code has been amply clarified in the Information Technology Act and there are other crimes which are committed hitherto in the physical world, which if done through the medium of internet using computers will be brought as cybercrimes and can be punished under the Indian Penal Code and to implement the same the term "electronic record" has been introduced in the IPC at relevant places to punishment the criminals.

Cyber Security Measures:

In India, there are many cybercrime laws enacted to stop this threat. Be it for the individual or the organization; these laws help to either bring down the number of cases or eliminate these digital crimes.

The simplest thing you can do to up your security and rest easy at night knowing your data is safe is to change your passwords. You should use a password manager tool like Last Pass, Dash lane, or Sticky Password to keep track of everything for you. These applications help you to use unique, secure passwords for every site you need while also keeping track of all of them for you. An easy way for an attacker to gain access to your network is to use old credentials that have fallen by the wayside. Hence delete unused accounts. Enabling two-factor authentication to add some extra security to your logins. An extra layer of security that makes it harder for an attacker to get into your accounts. Keep your Software's up to date.

Conclusion:

Cybercrime is becoming harder to stop as new technologies emerge, its impacts widespread and overwhelming financially. It's important to act now in order to slow its progress. Through increased awareness, improved laws which target cybercrime and by utilizing biometrics which greatly enhance security, the effects of cybercrime will be mitigated. As explored before, cyber criminals will only continue to find motivation in cybercrime when they are faced with such low risks. Governments' lack of funding and effort to take cybercrime seriously enough is only going to allow cybercrime to continue growing. The potentially shocking financial gains available will also only serve to motivate them even more. The fact that some statistics are a little out of date highlights limitations in accuracy but still serves the purpose in depicting the growth of cybercrime. Biometric technology is still developing and at the moment has certain limitations in regards to how accurately it can work or whether it's really an efficient way to go. Great areas for future research would be the growth in biometric technology and seeing how it will develop over time, as it should be a key area in securing one's personal information, not just for large organizations but for individuals at home as well. Cybercrime is only going to get worse over time unless preventive measures are taken to stop it, because at the moment, it's just too appealing of an option for criminals to say no to.

Cyber security is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. In practice, although technical measures are an important element, cyber security is not primarily a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Furthermore, what is known about cyber security is often compartmented along disciplinary lines, reducing the insights available from cross-fertilization. The cyber security problem will never be solved once and for all. Solutions to the problem, limited in scope and longevity though they may be, are at least as much nontechnical as technical in nature.

SOCIAL SECURITY THROUGH FIVE YEAR PLANS

By

—Dr. T. VIJAYA BHASKARA REDDY,
Principal, Aurora's Legal Sciences Academy
Hyderabad

Immediately after the commencement of the Indian Constitution, Planning Commission was set up in March, 1950 and through which Five Year Plans were formulated. All the Five-Year Plans emphasized the need for Social Security Schemes to achieve the Constitutional goals in establishing Social Justice and removing inequalities in the Indian Society. The First Five Year Plan showed special attention to labour problems in providing basic needs of worker for food, clothing and shelter.

The First Five Year Plan has two main objectives:

(1) A better standard of life for the people, and

(2) Social Justice.