An Analytical Study of Cyber Crimes: Issues, Challenges and Laws

Ms. Suman Madan

Asst. Prof(IT), JIMS, Sec-5, Rohini, Delhi

Ms. Neha Goel, Mr. Vijay Kumar

Research Scholar, JIMS, Sec-5, Rohini, Delhi

ABSTRACT

India is growing very fast and going forward to Digital India. For digitalization, Internet is very useful technology and it is growing very fast. So if the Internet is growing very fast, Cyber-Criminality is also growing fast. With the increase in technologies not only web servers are prone to cyber-crimes but these days even android and tablets are becoming a part of it. As tablets uses the same operating system used by Android devices there will be time coming soon in which attackers will also aim tablets. With time these attackers are aiming at vast area so that more number of users gets effected. By attacking it means that stealing personal information of the user of that device i.e. username, passwords, account details, political details, etc. The control on the cyber-crimes is totally dependent on analysis of their behaviour as well as on the understanding of their impacts over various levels of society. Therefore, in this paper, a systematic understanding of cyber-crimes, IT act 2000 and their impacts over various areaswith the future trends of cyber-crimes areanalysed.

KEYWORDS

Cybercrime, Security,information technology act, cyber attacks, Cyber Safety, cyber prevention and detection

INTRODUCTION

Cyber-crime is the crime which can be done with the help of the computer system. In this living world crime happens every day and we know that every country attacks on other countries. There are many hackers who attack on different industry and thus increasing the cyber-criminality or cyber-crime. Cyber-Criminality is stealing your data by unauthorised access from any computer and also hijacking your computer. Here is the need of securing today`s world and we need to secure our world from the attacker`s or the hacker`s.It has been observed from the data of last few years that the rate of cyber-crimes are increasing with every year instead of it being reduced which means with every year more people are becoming a part of crime. Conservativeestimates in research show cybercriminal revenues worldwide of at least $1.5 trillion – equal to the GDP of Russia. If cybercrime was a country it would have the 13th highest GDP in the world, according to thereport [1]. Figure 1 shows the chart which shows the increase in crimes in last few years [2].

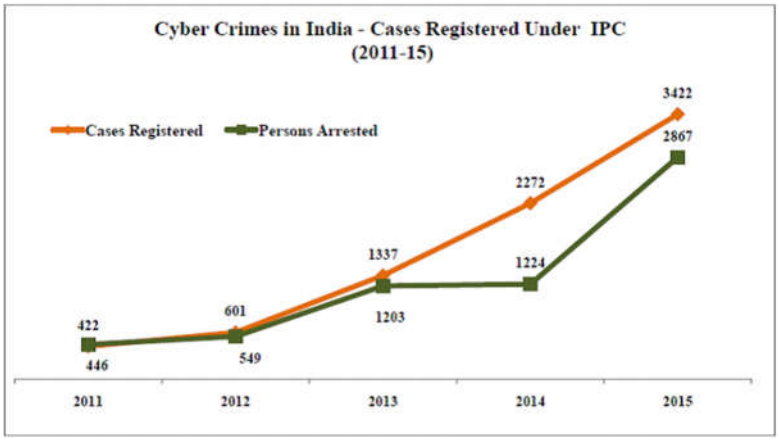

Fig:1 Cyber Crimes in India[2]

As defined by Joseph Migga Kizza [3] cyber security has 3 elements:

i. ***Integrity:*** It is authenticating the information i.e. whether the information is real (actual information) or unaltered, source from where the information is gathered is trustworthy or not. It is also important to ensure that the data must not be altered by anyoneexcept those who have access to the data.

ii. ***Confidentiality:*** Confidentiality of data means making sure that the data is secured and is not in the hands of someone wrong who is capable of or is willing to damage the original data with any kind of mind-set. Different measures are taken to ensure the security of data and also to avoid the data from reaching wrong hands. All the authorised people should have accurate knowledge of how to remain safe from data misuse and how to guard their files from unauthorised users.

iii. ***Availability***: All the required software, hardware, internet connectivity for updating of software should beeasily available with those who have access to the files and have the keys of cryptographic files. Also it should beensured that the data is available to those who have complete access to the data.

WHY CYBER SECURITY IS MUCH NEEDED

The Internet space or cyber space is growing very fast and as the cyber crimes. Following are few points which highlights need of cyber security [7-8]:

i. ***Mobile Devices and Apps:***Growth of mobile devices is increasing very fast. Nowadays almost every house has at least one smart phone which therefore increase the security risks as the attackers get one more network to attack on. As technology is increasing day by day attackers are also adapting new techniques to attack on such devices. All old technologies are merging with new features/technologies and thus resulting in development of new ways. Which increase the cyber security in every aspect and making the use of tablets/smart phones somewhat risky.

ii. ***Social Media Networking:***Social media has become a very common channel for communication for people residing far away at different places. More people are getting engaged in the medium of social media both for contacts and for daily entertainment. It is also seen that many use social media for updating their daily activities which has resulted in many different crimes. In past years it has been seen that number of accounts on different social media has increased widely. For the safety of users it is important for the companies to look after the policies used for the security of an individual engaged with them. If such step are not taken in proper manner then the number of crimes on social media will increase resulting in Individuals data being at risk.

iii. ***Protect Systems rather information***:These days everyone is trusting online sources more than anything for storing their important data as they feel that data stored online will not be lost and will be secure. For this reason it is important to protect the data of thousands of individuals who trust online sources for their data. It is important to secure the systems in which the data is being saved and it is most important to save the data stored within these systems. The companies as well as the users of the product of that company are requesting for strict policies for better security of the systems and the data stored in the system of large number of individuals.

iv. ***Everything Digital can bePhysical:***Doing the work manually takes double the time as compared to the work done using technology or rather we can say that if the work is done using computers it can be done in less amount of time. Because of this reason everyone is slowly and gradually moving towards digital method of doing work from manual work. Maintaining files, making notes, drawing of pictures, etc. everything can be done digitally and thus increasing thedependency on digital world will automatically increase the digital crimes i.e. cybercrimes. When cybercrimes will increase it is understood that the data of people for which they are using digital access is also not safe and security of user's data is the most important concern.

CATEGORIES OF CYBER CRIME

Generally the cyber crimes are categorized as follows:

i. **Data Crime :**Data Crime includes three things i.e. Data Interception, Data Modification and Data Theft.

a) *Data Interception:* An attacker generally do active or passive sniffing of data streams to or from a target in order to gather information. In this type of attack, the attacker is mostly not the intended recipient of the data stream. [3].

b) *Data modification*:It is possible only when security of data or file is not kept in mind and taken as a primary goal. Privacy of communication is very important which ensure that data cannot be modified or changed using any means. In this type of attack an unauthorized third party on the network interferes the victim's data and makes modifications intentionally before the data is further retransmitted.

c) *Data theft*:It is the term which is used to refer to a situation when data is illegallycopied from any type of source. Mainly the information which is stolen includes passwords, usernames, bank account details or other corporate details.

ii. **Access Crime :** These kinds of crimes can be further categorized:-

a) *Unauthorized Access:* Thedocuments when accessed by someone for whom that document is not meant to, it is called unauthorized access. There can be a case that when a document is accessed by someone not trust worthy, the user can makeundesired changes in thedocument.

b) *Virus Dissemination*: Malicious software that attachesitself to other software. Virus, worms, Trojan Horse, Time Bomb, Logic Bomb, Rabbit and Bacterium areexamples of malicious software that destroys the system of the victim.[4]

iii. **Network Crime:**Network crime can betermed as network interferences.Interfering thenetwork's functionality by transmitting, damaging, inputting, deleting or any other kind of interference in network data.

iv. **Related Crimes:** Not only the person who commits the crime is guilty but also who person who in any form is involved in the crime. There are three ways in which another person may get involved in the crime. First, if someoneelsecommitted the crime on behalf of that person. Second, if a person provided any kind of assistance or sources to the one who committed the crime. Third, someone who has prior information about the crime to take place.

TYPES OF CYBER ATTACKS& CYBER SECURITY

Following are thecommon types of cyber attacks[4,9-12]:

i. Worms:It is a malicious software program which infect other system and stay in the system which is affected. To affectanunaffected system it used a part of Operating System which is not visible to the user and are automatic.
ii. Viruses:It a malicious software program which is installed in the system in such a manner that the user will not be able to detect it. Virusesspread from onefile to another effecting others files and documents.
iii. Trojan Horse:It is a virus which is designed to get access to the system of the user on which this virus is installed. The user do not get to know that some virus is residing in his/her system.
iv. Bots:It is designed to effect the host and gets connected to aserver which acts as a commander i.e. which gives commands to this virus about the tasks it has to perform on the system it is residing in.
v. Unwanted Programs:These are the programs that areinstalled in the user's system without thepermission of the user.
vi. Phishing and Identity Theft:It is an attempt to steal or gather all the personal information of the user such as username, passwords, bank account details or credit card details.
vii. Spyware:It is an unwanted software which steals the data of internet usage by the user. It is considered as a malware.
viii. Cyber Vandalism:It is referred to something in which a websitecontents aredestroyedintentionally.

There are several types of computer securities that are completely based on protecting from different types of viruses. Table 1 shows common type of cyber securities.

Table 1: Types of Security

Type	**Description**
Network Security	Common type of computer security which deals with security of network. Protection from viruses, and many other threats from the internet. Hackers can pretend to be authorised user in order to get the access of the data which is secured and is not available to all.
Data Security	Security of different kind of data which are stored in the system either via hardware or software. Data can beusernames, passwords or bank details. It affects confidentiality, integrity and availability.
System Security	It refers to many malicious codes of software which can damage the security of a system. There are some software who secretly transfer virus in the system and thus effecting the security, stealing confidential data from the system, etc.

CYBER LAW PROVISIONS IN INDIA

Cyber crimes involves criminal activities which may besimple in nature liketheft, fraud, forgery, defamation and mischief, all of which aresubject to the Indian PenalCode. Theabuse of digital solutions has also given birth to a range of new age crimes that areaddressed by the Information Technology Act, 2000. Table 2 highlights few common offences with corresponding sections in IT act[5].

Table2: IT Act 2000 – Penalties, Offences

Section	Offense
43	Penalty and compensation for damage to computer, computer system, etc.
65	Tampering with computer sourcedocuments
66	Hacking with computer system
66A	Punishment for sendingoffensivemessages through communication services
66C	Identity theft
66D	Punishment for cheating by impersonation by using computer resource
66E	Punishment for violation of privacy
66F	Cyber terrorism
67	Punishment for publishing or transmitting obscenematerial in electronic form
67B	Publishing materialdepictingchildren in sexuallyexplicit act
69	Failure to decrypt data
70	Attempting to access of secure system
71	Misrepresentation

REMEDIES TO DECREASE COMPUTER RELATED OFFENCES

The key to the security from Cyber-Crime is prevention. There are many ways to protect our self from the cyber-crime. Always try Surfing the safe internet and avoid to visit theinappropriatewebsites which contains themalware or Hijack. We are well familiar nowadays with ransom ware virus, this virus blocks your precious data or information and ask for money to unlock your content. So always use the antivirus with updated database. It is always better to take certain precautions while working on thenet, some are strongly recommended[13,15]:

a) Use strong id/passwords and do not keep it same for all the accounts you have. Also do not write them anywhere as the place you are writing can also become cyber-attack victim.
b) Use network firewalls.
c) Keep backup of all your important data prior to any of the attacks through virus or any other medium.
d) Regularly update your operating system and antivirus.
e) Do not enter any of your bank details on thesites that are not secured, otherwise there can bechances of misuse of your data.
f) Before clicking on any of the link or emails know the origin of the same. Do not click any of the link which is not recognised by you.
g) Keep your social media sites private.
h) Do not store any of the personal information in your mobile devices and don't leave your mobile devices unattended.
i) Turn off your computer systems when not in use.
j) Encrypt your most private data to keep it secure and totally avoiding the chance of misuseeven if anyone who is not trustworthy have this information.

IMPACT OF CYBER CRIME

i. Social Impact: Attackers have found many different ways of attacking people on social media as they areaware of dependency of individuals on it. Attackers havestarted following individuals through the information on social sites update through them and thus harming them[5-6].

ii. Impact on Teenagers& Youth: Teenagers are becoming victim of cyber-crime via cyber bullying. As teenagers are moreinvolved in social media and indulging with new people, they are becoming easiertarget for such kind of activities Mostly girls are affected in it. Cyber bullying is basically when someonereceivessomethingnegative in the form of pictures, images, comments or messages from some other person. Mostly the users of Facebook, Twitter, Instagram and many more such social media applications are affected through cyber bullying.

iii. Impact on Business: Now a days E-Commercesites have become a boom and with increase in these cyber-crimes people are afraid of internet dealing and sharing their personal information on web. This has affected the business of many organisations and thus reducing thesales.Not only business on largescales become victim of cyber-attacks or face drawbacks of their customers being a part of cyber-attack but even business on small scale also face various problems and losses because of it.

iv. Impact on Consumer Trust: Thecyber-attackers intrude into other's space and try and break the logic of thepage, theend customer visiting theconcernedpage will befrustrated and discouraged to use the said site on a long term basis. Thesite in question is termed as thefraudulent, while the criminal masterminding the hidden attack is not recognized as theroot cause. This makes thecustomerlose confidence in the said site and in the internet and its strengths.

FUTURE TRENDS

Thebiggest concern is that now internet is becoming part of everything and people and getting dependent on it. Even money transactions are now being done through internet and this will eventually increase the cyber-crimes. Also it is very important to secure government sites from these attacks as large population is associated with it. Most of the organizations will adopt online methods for all work of the organization for theease of individual and organization. They will be moreactive about the security of the online portal by adapting more security models. Attackers will take advantage of thedependency on the social media and violate all the rules that are required to befollowed.

It is very easy to involve individuals in fake things by bribing them with attractive offers like providing goods in very cheap rate and thus making them to enter all their personal details or by using the tools which store the details they enter. Cyber attackers will always aim for those who areeasy to attack.

In future Memory Scrapping will be on thepeak. This mostly target on the personal data of individual likecredit card details, passwords, etc. This is becoming successful because they have get around the security PCI/GLBA/HIPAA/ETC. This security ensures that data should be in encrypted form during transmission and then this data is decrypted on the system and stored in the memory till the process is alive.

CONCLUSION

As the world is changing new technologies are coming in market day by day. There are many advantages and disadvantagesattached with everything. So, with new evolving technologies the advantage is that things are becoming easier but thedisadvantage is that the attackers are also getting updated and finding new ways of committing the crimes related to technologies. Cyber-crimes are increasing very fast and to protect ourselves from such

crimes there are various measures that need to befollowed. People need to beeducated so that they can beaware of theconsequences of cyber-crimes and how to protect them from it. Being updated is the best way to be safe from crimes.If the technologies are getting updated many other things are also changing its style. Moresecurities are arriving in market, more laws are being passed day by day so that there is no crimeleft related to cyber-attack which do not have any justice. Also already existing laws are being modified according to new technologies and ways of the attack.

REFERENCES

[1] https://www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/

[2] ArunPrabhudesai, "Cyber Attacks In India", 2011

[3] Kizza J. M., Guide to Complete Network Security,4thEdition, Springer International Publishing, ISBN:978-3-319-55605-5 (2017).

[4] Virus Glossary(2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml

[5] Tonge A. M., Kasture S. S., Chaudhari S. R., Cyber security: challenges for society-literature review, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, 12(2), 67-75 (2013).

[6] Dunn M., The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP), International Journal for Critical Infrastructure Protection, 1 (2/3), 58-68 (2005).

[7] Agarwal K., Dubey S. K., Network Security: Attacks and Defence, International Journal of Advance Foundation and Research in Science&Engineering (IJAFRSE), 1(3), 8-16 (2014).

[8] http://computernetworkingnotes.com/networksecurity-access-lists-standards-and-extended/ typesof attack.html.

[9] Homer J., Zhang S., Ou X., Schmidt D., Du Y., Rajagopalan S. R., and Singhal A.. Aggregatingvulnerability metrics in enterprisenetworks using attack graphs, Journal of Computer Security, 21(4), 561–597 (2013).

[10] Zhuang R., DeLoach S. A. and Ou X., Towards a theory of moving targetdefense, Proceedings of the First ACM Workshop on Moving TargetDefense, ACM, 31–40, (2014).

[11] Cerrudo C., AnEmerging US (and World) Threat: CitiesWideOpen to Cyber Attacks; retrieved from https:// ioactive.com/pdfs/IOActive_HackingCitiesPaper_ CesarCerrudo.pdf, accessed on 30.09.2017.

[12] Stewart J. N., Advanced Technologies/Tactics Techniques, Procedures: Closing the Attack Window and Thresholds for Reporting and Containment, Best Practices in Computer Network Defense: Incident Detection and Response M. E. Hathaway (Ed.) IOS Press, 2014.

[13] PrakharGolchha, Deshmukh R. and Lunia P., A Review on Network Security Threats and Solutions, International Journal of Scientific Engineering and Research (IJSER), 3(4), 2347:3878 (2015).

[14] Emerging Trends in Computer Science and Information Technology, Shabd Publications, Bhopal, India, ISBN: 978-93-85145-05-6.

[15] Alpana, Malhotra S., Cyber Crime –Its types analysis and prevention Techniques, International Journal of Advanced Research in Computer Science and SoftwareEngineering, ISSN-227128X, 6(2), 145-150 (2016).