International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Crime and Cyber Security

Gajendra Kumar Malviya

Associate Professor, Sociology, Government PG College, Jhalawar, Rajasthan, India

ABSTRACT

The crime that involves and uses computer devices and Internet, is known as cybercrime. Cybercrime can be committed against an individual or a group; it can also be committed against government and private organizations. It may be intended to harm someone's reputation, physical harm, or even mental harm. Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft. Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access. All sorts of data whether it is government, corporate, or personal need high security; however, some of the data, which belongs to the government defense system, banks, defense research and development organization, etc. are highly confidential and even small amount of negligence to these data may cause great damage to the whole nation. Therefore, such data need security at a very high level.

KEYWORDS: *cyber, crime, security, internet, computer, nation, government, banks, corporate*

How to cite this paper: Gajendra Kumar Malviya "Cyber Crime and Cyber Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.1978-1986, URL: www.ijtsrd.com/papers/ijtsrd49888.pdf

IJTSRD49888

INTRODUCTION

Cyber crimes are increasingly becoming social engineering, where cyber criminals invest resources and time to gain knowledge about technical and scientific aspects of cyber security and because of that the term "cybercrime" is often confused with the term "cyber security". Even though the two are extremely different and belong to different areas of expertise, yet they are interrelated with each other. Cyber crime is a crime that involves the use of computer devices and the Internet. It can be committed against an individual, a group of people, government and private organizations. Usually it is intended to harm someone's reputation, cause physical or mental harm or to benefit from it, for example, monetary benefits, spreading hate and terror etc. As happened in 1998, a group of Tamil guerrillas, known as Tamil Tigers, sent over 800 e-mails to Sri Lankan embassies. [1,2] The mails read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities identified it as the first known attack by terrorists against a country's computer systems. The main principle of cyber crime law is punishing unauthorized access or illegal use of computer systems and the internet with criminal intentions, so that damage and alteration of systems and data on it can be prevented. However, the largest threat of cybercrime is on the financial security of an individual as well as the government.[3,4]

Cyber security is a technique to protect computers, networks, programs, personal data, etc., from unauthorized access and threats. It is an activity by which information and other communication systems are protected and defended against the unauthorized use or modification or exploitation of the device. [5,6] Cyber security is also called information technology security. It includes the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that can cause damage to them or exploit them in any way.[7,8] Basically cyber security is a technical approach to secure systems from such attacks. Good cyber security recognizes all the vulnerabilities and threats a computer system or network contains. It then identifies the cause of such vulnerabilities and fixes those vulnerabilities and threats and secures the system. Strong cyber security programs are based on a combination of technological and human elements.[9,10]

There are certain aspects on which cyber crime and cyber security can be differentiated upon, they are:

- Types of crimes: In cyber security, the kinds of crimes are where a computer software or hardware or computer network, is the main target (ransomware, viruses, worms, distributed denial of service attacks etc).

In Cyber crimes, the crimes are where an individual or a group of individuals and their data is the main target. Governments and organizations can also be the targets of cyber crimes (cyber bullying, hate speech, child pornography trafficking, trolling).[11,12]

- Victims: Victims in these two fields are also different. In cyber security, victims are governments and corporations whereas, in cyber crimes, the range of victims is rather broad as victims can extend from individuals, families, organizations, governments and corporations.
- Area of Study: Both these fields are studied in different areas. Cyber security is dealt with under Computer science, computer engineering, and information technology. Coding, networking and engineering strategies are used for making networks more secure.

On the other hand, cyber crimes are dealt with under Criminology, psychology, sociology. Basically, it is the theoretical understanding of how and why crime is committed and how it can be prevented.[13]

For a strong cyber security system certain elements are needed. The elements are as following:

- Application security: Applications play an essential role in business ventures; that is why every firm needs to focus on web application security. Web application security is important in order to protect customers, their information and interests. Application security helps in thwarting any attempts to violate the authorization limits set by the security policies of the computer system or networks.
- Information security: Information includes business records, personal data, customer's data, intellectual property etc; hence, it is important for a corporation to have strong cyber security for information to prevent its leakage.[14,15]

Information security involves safeguarding sensitive information from illegitimate access, usage, or any other kind of damage. This also ensures that the important data does not get lost when any issue like natural disasters, malfunction of system, theft or other potentially damaging situation arises. The characteristics defining information security are confidentiality, integrity and availability. Information security also includes Data Confidentiality, Data integrity, Data availability, and Data authenticity.

Network Security: Network security consists of protecting the usability and reliability of network and data. A network penetration test is conducted to assess the vulnerabilities in a system and network.

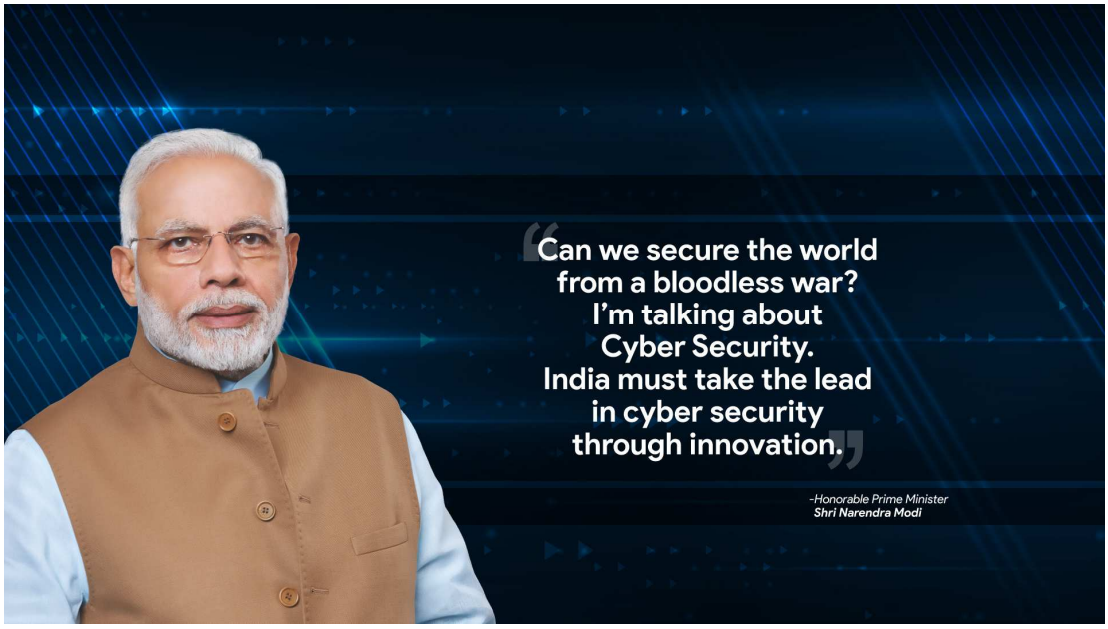
It refers to broad range security policies for thwarting and monitoring unauthorized access, misuse, damage to a computer system and other network systems. Network security extends coverage to diverse computer networks, surrounding private and public communication systems among corporations and organizations.[16,17]

- Disaster Recovery/ Business continuity planning: Business continuity planning (BCP), also known as disaster recovery, is about being prepared for any kind of interference or cyber threat by identifying threats to the systems on time and analyzing how it may affect the operations and methods to counter that threat.
- Operational security (OPSEC): Operations security is used to protect organization functions. It identifies important information and assets to track down threats and vulnerabilities that exist in the functional method.
- End-user education: It is important for an organization to train their employees about cyber security because human error is one of the major causes of data breaches. Every employee should be aware of the common cyber threats and should have the knowledge to deal with them.

Training will allow management to accustom themselves with system users and threats to it and user training will help in eliminating resistance to change and advancements and lead to user scrutiny on a closer level.[18,19]

Leadership commitment: It is important to have leadership commitment in organization and corporations in order to have a strong cyber security program. Without having the leadership in the team it is complicated to develop, implement and maintain the cyber security processes.

Discussion



The cyber crimes may be broadly classified into four groups. They are:

Crime against the Individuals

Crimes against the individual refers to those criminal offences which are committed against the will of an individual to cause certain harm to them like physical or mental harm. For example assault, harassment, kidnapping, and stalking etc. but in cyber crimes the nature of crimes against individual changes a little bit and takes the form of cyber stalking, pornography, cyber bulling, child abuse, fraud, cyber threats etc.[20,21] Such as cyber defamation is committed to cause harm to the reputation of an individual in the eyes of other individuals through the cyberspace. A few cyber crimes against individuals are:

1. Harassment via electronic mails.
2. Dissemination of obscene material.
3. Cyber-stalking.
4. Defamation.
5. Indecent exposure.
6. Cheating.
7. Unauthorized control/access over computer system.
8. Email spoofing.
9. Fraud.[22,23]

Crime against Property

The second category of cyber crime is that of cyber crimes against property. With the growth of international trade, businesses and consumers are increasingly using computer and the internet to create, transmit and store information in the electronic from instead of traditional form. This has ultimately lead to certain cyber offences which affect a person's property. These types of cyber crimes include cyber vandalism to steal information of other organizations or to steal someone's bank details, use software to gain access to an organization's website etc. This is similar to instances of a criminal illegally possessing an individual's bank or credit card details. In cyber crime, the hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use any kind of malicious software to gain access to a web page with confidential information. These types of crimes include vandalism of computers, intellectual property crimes (Copyright, patented, trademark etc), online threatening etc. Cyber crimes against property include:

1. Computer vandalism.
2. Transmitting virus.
3. Net-trespass.
4. Unauthorized access / control over computer system.
5. Internet thefts.
6. Intellectual Property crimes
7. Software piracy.
8. Copyright infringement.
9. Trademark infringement.

Crime against Governments or Organizations

There are certain cyber crimes committed to threaten the international governments or organizations. These cyber crimes are mainly committed for the purpose of spreading terror among people of a particular country. [24,25]

The instigators or perpetrators of such crimes can be governments of enemy nations, terrorist groups or belligerents etc. Cyber crimes against Government include cyber attack on the government website, military website or cyber terrorism etc. In these kinds of cyber crime, cyber criminals hack governments or organization's websites, government firm, and military websites and then circulate propaganda or threats or rumors. These cyber crimes are known as cybercrimes against Governments or Organizations. Following are the few examples of crime against Governments or Organizations:

1. Unauthorized access / control over computer system.
2. Cyber terrorism against the government or organization.
3. Possession of unauthorized information.
4. Distribution of Pirate software.

Crime against Society

Those cyber crimes which affect the society at large are known as cyber crimes against society. These unlawful acts are committed with the intention of causing harm or such alterations to the cyberspace which will automatically affect the large number of people of society. The main target of these types of crimes is public at large and societal interests. [26,27] The cyber crimes against society include the following types of crimes:

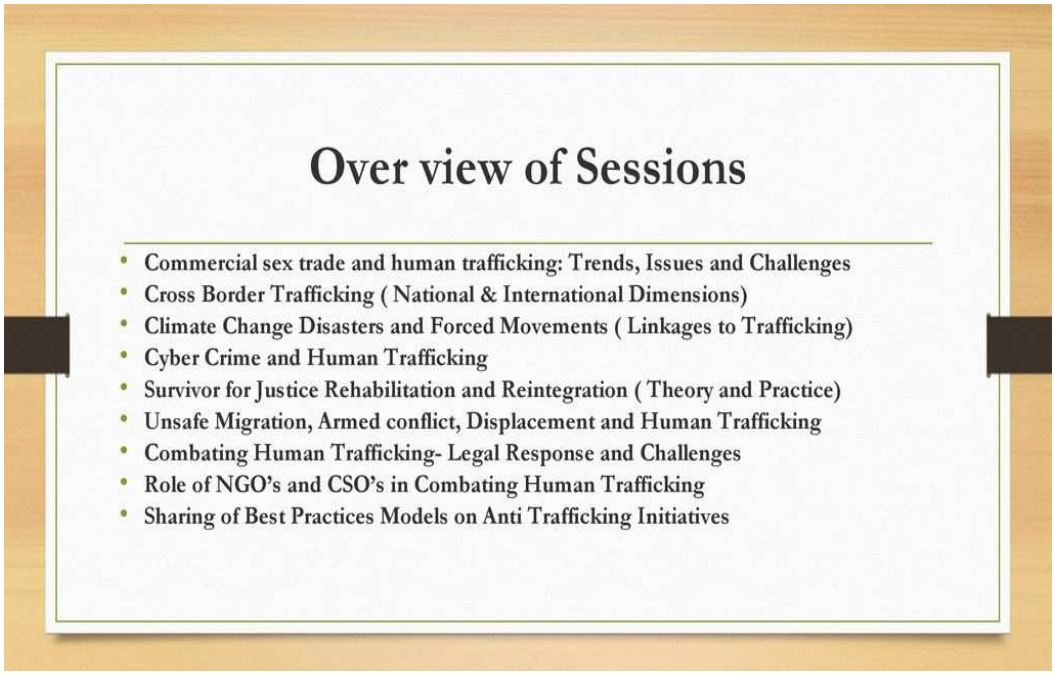
1. Child pornography.
2. Indecent exposure of polluting the youth financial crimes.
3. Sale of illegal articles.
4. Trafficking.
5. Forgery.
6. Online gambling.
7. Web jacking.

Results

Protect Yourself

- Taking the right security measures and being alert and aware when connected are key ways to prevent cyber intrusions and online crimes. Learn how to protect your computer, network, and personal information.
- Understand Common Crimes and Risks Online
- Business email compromise (BEC) scams exploit the fact that so many of us rely on email to conduct business—both personal and professional—and it's one of the most financially damaging online crimes.
- Identity theft happens when someone steals your personal information, like your Social Security number, and uses it to commit theft or fraud.
- Ransom ware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
- Spoofing and phishing are schemes aimed at tricking you into providing sensitive information to scammers.
- Online predators are a growing threat to young people.
- More common crimes and scams[28]

Our adversaries look to exploit gaps in our intelligence and information security networks. The FBI is committed to working with our federal counterparts, our foreign partners, and the private sector to close those gaps.



These partnerships allow us to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. The FBI fosters this team approach through unique hubs where government, industry, and academia form long-term trusted relationships to combine efforts against cyber threats.

Within government, that hub is the National Cyber Investigative Joint Task Force (NCIJTF). The FBI leads this task force of more than 30 co-located agencies from the Intelligence Community and law enforcement. The NCIJTF is organized around mission centers based on key cyber threat areas and led by senior executives from partner agencies. Through these mission centers, operations and intelligence are integrated for maximum impact against U.S. adversaries.

Only together can we achieve safety, security, and confidence in a digitally connected world.

Whether through developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships in our communities, the FBI continues to adapt to meet the challenges posed by the evolving cyber threat.[29]

The FBI has specially trained cyber squads in each of our 56 field offices, working hand-in-hand with interagency task force partners. The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents. With cyber assistant legal attachés in embassies across the globe, the FBI works closely with our international counterparts to seek justice for victims of malicious cyber activity.

The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. Using such complaints, the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cyber crime. Cy Watch is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

Conclusion

Malicious cyber activity threatens the public's safety and our national and economic security. The FBI's cyber strategy is to impose risk and consequences on cyber adversaries.

Our goal is to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. To do this, we use our unique mix of authorities, capabilities, and partnerships to impose consequences against our cyber adversaries.

The FBI is the lead federal agency for investigating cyber attacks and intrusions. We collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are.

Cyber security can be considered as a set of guidelines and actions intended and needed to prevent cybercrime but cyber security is not only limited to that. The two types of problems differ considerably in terms of what happens and who the victims are, as well as the academic areas that study them. Therefore, the two, cyber security and cyber crimes, must be considered as separate issues, with different safeguards designed to address the different privacy and security issues of each.

All sorts of data whether it is personal, governmental, or corporate need high security. Some of the data, which belongs to the government defense system, scientific research and developments, banks, defense research and development organization, etc. are highly confidential and even small amount of

negligence to these data may cause great damage to the whole nation or society at large, therefore, such data need security at a very high level.

Hence, cyber security is all about protecting government, organizations and corporate networks, intending to make it difficult for hackers to find weaknesses and exploit them or threaten them. Cybercrime, on the other hand, tends to focus more on individuals and families online. It is highly needed that the top leaders of an organization or government should invest in the cyber security measures to make it strong and impenetrable. [30]

References

[1] Cyber Crime and Cyber Security; tutorials point; Date of Access: 30.10.2019 <https://www.tutorialspoint.com/fundamentals_of_science_and_technology/cyber_crime_and_cyber_security.htm>

[2] The difference between cyber security and cybercrime, and why it matters by Roderick S. Graham; The Conversation; Dated: 19.10.2017; Date of Access: 30.10.2019 < https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654>

[3] Understanding the Difference between Cyber Security and Cyber Crime; Privacy International; Date of Access: 30.10.2019 <https://privacyinternational.org/explainer-graphic/2273/understanding-difference-between-cyber-security-and-cyber-crime>

[4] Elements of cyber security by Robert Roohparvar; InfoGuard Cyber Security; Dated: 02.03.2019; Date of Access: 30.10.2019 < http://www.infoguardsecurity.com/elements-of-cybersecurity/>

[5] Elements of Cyber Security; Cross Domain Solutions; Date of Access: 30.10.2019 < http://www.crossdomainsolutions.com/cyber-security/elements/>

[6] Chapter III: Meaning, Concept and Classification of Cyber Crime; Shodhganga; <https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11_cha%5bpter%203.pdf>

[7] Types of cyber crime; Panda Security; Dated: 20.08.2018; Date of Access: 30.10.2019 < https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/>

[8] Cyber Crime Vs Cyber Security: What Will You Choose?; Europol; Date of Access: 30.10.2019 <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose>

[9] Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) (eds) Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York.

[10] Bowker, Art (2012) "The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century" Charles C. Thomas Publishers, Ltd. Springfield.

[11] Brenner, S. (2007) Law in an Era of Smart Technology, Oxford: Oxford University Press

[12] Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology (pp. 49–64). New York: Springer (ISBN 978-1-4614-5217-1)

[13] Chang, L.Y. C. (2012) Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait. Cheltenham: Edward Elgar. (ISBN 978-0-85793-667-7)

[14] Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber world", in M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.

[15] Csonka P. (2000) Internet Crime; the Draft council of Europe convention on cyber-crime: A response to the challenge of crime in the age of the internet? Computer Law & Security Report Vol.16 no.5.

[16] Easttom, C. (2010) Computer Crime Investigation and the Law

[17] Fafinski, S. (2009) Computer Misuse: Response, regulation and the law Cullompton: Willan

[18] Glenny, M. DarkMarket : cyberthieves, cybercops, and you, New York, NY : Alfred A. Knopf, 2011. ISBN 978-0-307-59293-4

[19] Grabosky, P. (2006) Electronic Crime, New Jersey: Prentice Hall

[20] Halder, D., & Jaishankar, K. (2016). Cyber Crimes against Women in India. New Delhi: SAGE Publishing. ISBN 978-9385985775.

[21] Jeremy Bob, Yonah (2021) "Ex-IDF cyber intel. official reveals secrets behind cyber offense". The Jerusalem Post

[22] Branch, J. (2020). "What's in a Name? Metaphors and Cybersecurity." International Organization.

[23] Costigan, Sean; Hennessy, Michael (2016). Cybersecurity: A Generic Reference Curriculum (PDF). NATO. ISBN 978-9284501960.

[24] Fuller, Christopher J. "The Roots of the United States' Cyber (In)Security," Diplomatic History 43:1 (2019): 157–185. online

[25] Kim, Peter (2014). The Hacker Playbook: Practical Guide To Penetration Testing. Seattle: CreateSpace Independent Publishing Platform. ISBN 978-1494932633.

[26] Lee, Newton (2015). Counterterrorism and Cybersecurity: Total Information Awareness (2nd ed.). Springer. ISBN 978-3319172439.

[27] Montagnani, Maria Lillà and Cavallo, Mirta Antonella (26 July 2018). "Cybersecurity and Liability in a Big Data World". SSRN.

[28] Singer, P. W.; Friedman, Allan (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. ISBN 978-0199918119.

[29] Wu, Chwan-Hwa (John); Irwin, J. David (2013). Introduction to Computer Networks and Cybersecurity. Boca Raton: CRC Press. ISBN 978-1466572133.

[30] M. Shariati et al. / Procedia Computer Science 3 (2011) 537–543. Enterprise information security, a review of architectures and frameworks from interoperability perspective