Research Paper
Impact Factor: 6.089
Peer Reviewed Monthly Journal
www.ijmdrr.com

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

CYBER VICTIMIZATION: A CONCERN FOR NATIONAL SECURITY AND CYBER DOMAIN

MD Asfak Abdulbhai Momin
Security Analyst – Field Officer, Atit Management Service Pvt. Ltd

Abstract
Cyber victimization is one consequence of technology use by world community. Cyber victimization is defined as experiencing aggressive behaviors via information and communication technologies, such as the internet, gaming consoles, and mobile phones. Experience of cyber victimization is hereby providing more details about the types of different victimization, technologies where victimization occurred. World is going on the digitalization or cash less transaction so multifold. Even the government and defense organization have experienced significant cyber losses and disruptions. The crime environment in cyber space is totally different from the real space that is why there are many hurdles to enforce the cybercrime law as real space law in any society. The present research paper explores about the concern of cyber victimization and its consequences upon national security of the nation.

Keywords: Cyber Victimization, National Security, Threat, Digital India

Introduction

In today's modern world, Cyber Security has been the main component of a state's National Security. According to United Nations Global Cyber security index (2017) India stands at number 23. Cyber security has a much dominance in India as India has world's largest biometric database (adhar), large campaigns of "Digital India", second largest mobile users in the world as well. For protecting all of the above things we need solid strategies and rules. Need such as making people aware about cyber domains, construction of well equipped anti cyber terrorism wing, Ethical Hacker postings in government departments, availing cyber security courses for students.

Cyber Victimization has been a growing concern for today's National security. Due to the Covid- 19 outbreak cyber crime has victimized more than 58% of users worldwide and an uptick in phishing email by cyber criminals have emerged. Unlike geographical boundaries cyber space and relevant system does not have any limitations. As it is borderless, protection of cyber security becomes more challenging now. Dependence upon the ICT for number of reasons such as booking a cab, booking flights, Money transfer lest to wide amount of information on the broadcast which makes it more vulnerable. Recent observations made by National cyber security coordinator, Dr Rajesh Pant which states in year 2019 cyber crimes caused around 1.25 trillion loss. It will gradually increase as country will move towards 5G and making other smart City initiatives. Such database shows us the loopholes pertaining in the country as with the population of 1.2 billion the amount of vulnerability also increases with the gradual increase the technology.

Cyber Threat and Sources

1- Malware – software to disrupt the computers.
2- Hacktivism- attacks which are socially and politically motivated.
3- Social Engineering- threat to users by clicking on the unknown links.
4- Spear Phishing- through e-mails, texts, tweets.

5- Router security- Border gateway protocol, hijacking
6- Denial of service- through blocking access to the website.

Such cyber threats have different sources like Nation States, Cyber Criminal Organization, Terrorists, DTOs, hackers / hacktivism. The main cyber players and their motive s can be identified through studying their players , are as follows:

1- **Cyber Criminals-** seeking money through banks and financial institutions.
2- **Cyber Terrorists-** through attacking on the assets and national infrastructure.
3- **Cyber Espionage-** using IT malwares to penetrate national and Military data's
4- **Cyber Hectivists-** Anonymous groups with social and political motives and agendas by messaging through specific campaigns.

Cyber attacks has many motives such as commercial gains through hacking banks, to penetrate in military and intelligence data to know their plans. Problems such as malware, phishing, cyber terrorism, social engineering, hacktivism are increasing with time.

Cases and Preface showing way to Cyber security
Recent cyber attacks in India Cosmos bank cyber attack, wanna cry (2017), Miraibotnet shows us the need of having a strong cyber industry in India where it could be tackled.

In addition to all such cyber attacks, recently a Chinese group named Red Echo was behind the cyber attack called Shadow pad which was on India's critical information infrastructure such as power systems, ports etc. It tells us the upcoming damages which could cause to a nation's security if neglected.

Laws such as IT Act 2000, National cyber police 2013 under which a secure cyber database ecosystem should be created. Government initiatives such as Cyber swachhata kendra, Cyber surakshit Bharat initiative have been there but still these are not able to address or reach to an extent where it should due to lack of cyber knowledge.

The internet should be considered as the interconnection of different networks which at some pace has given rise to the new E- crime methods. If one of the side shows the positive values the another shows negative which gives birth to the innovations to different crime patters and ways with the growth of e-crimes it also causes damage to firms, government, people. As such it could be considered that cyber crimes and its Victimization causes damage at a large and extensive way.

Following the different methods through which E-crimes are channelized:
Computerized Crimes: Use of electronic methods which can attack Security and data's for illegal means and fraud. E- crimes have became easy and fast with the advancement in the Information technology.

White Color Crimes: Crime committed by an individual with high respectability and status in the society for fraud and illegal means to obtain money. White collar crimes with the help of internet and computers have become easier and faster if we see the other side of the internet use. Every year large

number of people are Victimization with such crimes high rate which is caused by high profile individuals.

High Tech Crimes: Criminal activities which are penetrated by the use of computers. It also disturbs and violates the fundamental laws. These malicious activities take place due to hacking, money laundering, malware, harassment, identify theft.

Cybee Crimes: Criminal activities perused with the help of computers with an illegal aim or mind-set or stealing something with the use of internet could be termed as cyber crime. Hacking, phishing, spam, online sex pornography could be termed under it.

Cyber Terrorism: This new form of cyber crime could be considered something that is politically motivated and could be channelized as crimes against banking industry, power plants, military forms and data's as well.

Methods of E-Crimes/E-Victimization:

Hacking: Hacking is done through highly efficient programmers well know as Hackers. They enter into a particular computer system through illegal means which gets converted into crime if done with malicious purpose. With easy target's the objective of hacking is to enter and disband a security code and collect the information, get operation cods, operating system and many a times with means of damaging the national security as well.

Phishing: Phishing could be considered as a way to get the sensitive information through illegal means by getting password, database, monitor access, credit card details, through online modes by using different websites by illegal means. It could be defined as a method to get illegal data by authentic emails which are made available which phishing method. It generally creates an illusion identity and makes things transparent which looks real and data are shared by the other opponent, hence, the total information is collected and used for illegal work.

Spam: Spam could be termed as unwanted messages or e-mail over the internet world that too at large number of users that includes phishing, hacking, malware, used at a large scale to an extent for illegal means and fraud. Most common forms which spam include is of E- spam.

Factors of Victimization through E-Crimes:

1) **Financial E- Crimes:** Financial E-crimes are considered to be white collar crimes which takes place with the help of computer use more frequently and becomes a major factor affecting firms, banks, at national and international levels. It also harms economic and social sector through a huge loss of money.

2) **Political E-Crimes:** Theft of money, adultery, Terrorism which rests under the political e-crimes usually occurs with the help of internet connection which eventually turns into a big money loss. Use of Information technology is an easy way for the terrorist organisation to make further communication.

3) **Sexual E-Crimes:** Under such E-crimes the offender on the one side becomes active and results in such criminality. The data saved are than used for the abusive content.

1) ***Extortion:*** one of the forms where data are taken through different mode of computers and then girls are asked for money for their nudes and images which is results in extortion.
2) ***Child Abuse At Home****:* Another way through which initially seduction is done and then the child is abused through different ways which sometimes results in suicidal forms. Every year, many children become victim of such sexual predators worldwide.

3) ***Pornographic Websites****:* Through such sites the sexual content is delivered to the public. It could also be noticed that how such hype in the young age group sexually affects the generation and push them towards the animals on the internet. A proper supervision is needed for the blockage of such increasing and rapid e-crimes.

Steps to curb cyber victimization and enhance cyber security.

- **Network Security** -Data protection from internal and external attacks and also monitor and protect test security control. Network security can firmly help in reducing the threat of data loss, and also sabotage. Thus, it could be considered as a priority in effort to take care of any data.

- **Malware Protection –** Making of Anti malware defence which are related to mostly all business areas. Top areas of priority could be properly taken care of if protection of malware is considered and we'll maintain. A good antivirus tool can also be installed for any problems of E- crimes.

- **Monitoring -** There is a need to channelize monitoring and strategy and also frequently managing all ICT system, networks to keep things safer from the inner and outer attacks. Security with monitoring becomes crucial for any firm and individual for the sufficient tasks. Thus, a proper monitoring could help in reversing any threat that comes forward.

- **Incident Management –**There is a need to establish capacity building and disaster recovery capabilities. Also, to provide training to the field related personals. Only after doing the period stuff of making the Security assessment a way to curb the crime the incident management could also be used to eradicate and manage the crimes with time.

- **Secure Configuration-** Application of patches and all ICT Configuration systems is maintained. Necessary of building a base line for all ICT device is also necessary. Today every device could be detected easily and also a crime with such detection could arise and damage the code and Security, this making configuration codes for Security stuff becomes important.

- **User Education and Awareness-** There is a need to learn the policies and regulations with bit of awareness regarding such organisation systems that can boost things in a proper manner. With such a growing world it become necessarily have things in a right order where only Security comes at the preferential and priority.

India needs to make its computer environment more mature with new methods of cyber domain. Development of core skills which could decrease the cyber-Victimization in cyber security is the need of the hour. This paper addresses the situation, challenges and different dimensions of cyber security and also tends to show the need of our whether what could be done to uplift a Nation's Cyber Security.

Reference

1. Bauman, S. (2010): Cyberbullying in a rural intermediate school: An exploratory study. *J. Early Adolesc.* 2010, 30, 803–833
2. Britsch, B.; Wakefield, W.D. (1998): The influence of ethnic identity status and gender-role identity on social anxiety and avoidance in Latina adolescents. In Proceedings of the Paper Presented at the Annual Meeting on the American Educational Research Association, San Diego, CA, USA, 17 April 1998.
3. Brown F Christina (2014): 'Cyber Victimization in Middle School and Relations to Social Emotional Outcomes, *Computers in Human Behaviour,* 35 (6), pp 12-21
4. Connell, N.M.; Schell-Busey, N.M.; Pearce, A.N.; Negro, P. (2014): Badgrlz? Exploring sex differences in cyber bullying behaviours. Youth Violence Juv. Justice 2014, 13, 209–228
5. Huang, Y.; Chou, C. (2010): An analysis of multiple factors of cyber bullying among junior high school students in Taiwan. Comput. Hum. Behav. 2010, 26, 1581–1590
6. Raskauskas, J.; Stoltz, A.D. (2007): Involvement in traditional and electronic bullying among adolescents. Dev. Psychol. 2007, 43, 564–575.
7. Richardson, D.; Hammock, G. (2007): Social context of human aggression: Are we paying too much attention to gender? *Aggress.* Violent Behav. 2007, 12, 417–426.
8. Tushar P. Parick et al. (2017): 'Cyber Security: Study on Attack, Threat, Vulnerability' *International Journal of Research in Modern Engineering and Emerging Technology*, Vol 5, Issue 6, June 2017
9. Underwood, M.K.; Rosen, L.H. (2011): Gender and bullying: Moving beyond mean differences to consider conceptions of bullying, processes by which bullying unfolds, and cyber bullying. In Bullying in North American Schools; Espelage, D., Swearer, S., Eds.; Routledge: New York, NY, USA, 2011; pp. 33–42.
10. Wright F Michelle and Sebastian Wachs (2020): 'Adolescents' Cyber Victimization: The Influence of Technologies, Gender, and Gender Stereotype Trails, *International Journal of Environmental Research and Public Health,* 2020, 17, 1293.