CYBERCRIME: CERTAIN FORMS AND SOME SUGGESTIONS TO TACKLE CYBER CRIMES

Ms Babita Banga

Assistant Professor in Education, CCE, Landran, Mohali

Abstract

Cybercrime is a form of criminal behavior which uses any type electronic device through internet connection service which enables a criminal behavior being carried out, whether it involves an individual or a group of people and is able to transcend limitation from one country to another, in periods that are short and without reserved limitation. Cybercrime causes loss or damage to the equipment, data and information that involves a computer's software or processing; whether from a virus attack, invasion (unauthorized access and use) and information theft on a computer or electronic device that becomes the target. The present paper presents the review literature on cyber crime, certain forms of cyber offences and some suggestions and steps to tackle cyber crimes.

Keywords: *Cybercrime, Damage, Suggestions*

Introduction

Today's rapidity of science and technology is an undeniable fact. It has offered various advantages and benefit to everyone who make use of it. Likewise is the case for the utilization of the cyber world that is born from the advancement of science and technology. It has been given attention by the society today because of the many advantages that will be acquired, among them is to facilitate affairs and time saving. However, despite the advantages offered, it is still exposed to various risks and harmfulness for its consumers.

Cybercrime

Cyber consumers are also easily exposed to become victim to cybercrime carried out by irresponsible people (Ahmad Shawal, 2012). Cybercrime is a form of criminal behavior which uses any type electronic device through internet connection service which enables a criminal behavior being carried out, whether it involves an individual or a group of people and is able to transcend limitation from one country to another, in periods that are short and without reserved limitation (Anita & Nazura, 2004). Cybercrime causes loss or damage to the equipment, data and information that involves a computer's software or processing; whether from a virus attack, invasion (unauthorized access and use) and information theft on a computer or electronic device that becomes the target (Rusli, et.al, 2003).

Cybercrime that exists today is no longer confined only to the use of computer as a tool in committing crime, but instead, cybercrime today is also defined as crime which occurred in the internet or cyber world, which involves fraud and contriving trick (Anita and Azura, 2004). Group categorized as cyber criminal on the other hand is those having inverse thinking about the diversity of ICT usage (technodystopianism), which regards the cyber world as a platform to create wealth and pleasure. They use the cyber world to commit crime like hacking, transmit viruses, mailbomb, pornographic image, poison-pen letter and so on (Jalaluddin, 2008). Their targeted victims on the other hand, are generally irrespective of level of society, sex and age. But the victims are definitely those who had used the services in the cyber world for various purposes, like socializing, trading, doing a transaction and various other work affairs.

Review of literature on cyber crime

Jewkes (2006) analyses typologies of cyber crime in detail. He discusses on-line victimization, the social construction and policy implications of Internet crime, the dichotomous nature of cyberspace, the impenetrable anonymity of the virtual universe, and the challenges of regulation and control. Mcquade(2008) observes “Whereas crime statistics of traditional types have been falling in recent years, cyber crime has exploded in an environment where traditional law enforcement has been largely unprepared. “He starts out with a valuable addition to the discussion of the sociology of cyber crime: the concept of deviance of behavior in a new and rapidly changing field. The author also reviews the various types of cyber attacks and crimes .The psychology of cyber criminals and abusers is reviewed which also provides a very detailed classification for social engineering, and Donn Parker’s SKRAM (skill, knowledge, resources, access, motivation) model for assessing attackers. McQuade notes the difficulty in getting agreement on a profile for computer abusers, but does not address the changing style of attacks and attackers over time. Pornography, Hacking, Bullying, Cyber terrorism have been discussed by him in detail.

Duggal ((2009) provides a comprehensive overview of the cyber law scenario in India, provides recommendations for upgrading the current cyber law acts, and contextualizes these developments with respect to actual reported cases of cyber law in India. The author is a practicing advocate of the Supreme Court of India, and is a prolific writer and speaker. "Cyber law is important because it touches almost all aspects of transactions and activities concerning the Internet. Cyber law concerns everyone," Duggal begins. Drawing on the UNCITRAL law on e-commerce, the Indian government drafted the IT Bill of 1999 which was then implemented as the IT Act 2000 in October 17, 2000. It targets three existing areas of la contract, penal code, and evidence, and expands theprovisions of the Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, the Reserve Bank of India Act of 1934, and the Companies Act of 1956. There are several positive aspects of the IT Act 2000: it provides legal infrastructure for e-commerce transactions, recognizes electronic documents as legal entities, opens up business opportunities for digital certificate companies, paves the way for e-government transactions, and creates provisions against cyber crime. The author calls for more education and orientation for police officers on the intricacies of cyber crime; there was a case of police officers carrying away computer monitors during a raid in Mumbai, thinking they were the actual computers. Ghosh (2010) has addressed various issues as how multiple disciplines concurrently bring out the complex, subtle, and elusive nature of cyber crimes, how cyber crimes will affect every human endeavor, at the level of individuals, societies, and nations how to legislate proactive cyber laws, building on a fundamental grasp of computers and networking, and stop reacting to every new cyber attack, how conventional laws and traditional thinking fall short in protecting us from cyber crimes

Certain forms of cyber offences

- **Cyber Stalking**: According to Wikipedia, "Cyber Stalking is the use of the internet or other electronic means to stalk or harass an individual, a group of individuals or an organization. It may include the making of false accusations or statements of the fact, monitoring, making threats, identity theft, damage to data or equipment, and the solicitation of minors for sex, or gathering information that may use to harass (Cyber Stalking 2013).
- **Cyber Defamation:** It occurs when someone posts defamatory matter about someone on website or sends emails containing defamatory information to all that of person's friends (Agarwal 2013). 71.7% had been defamed in the cyber space and also in offline due to cyber defamation as surveyed by CCVC (Center for Cyber Victim Counseling) report 2010 (Halder and Jaishankar 2010).
- **Email Spoofing:** It is sending email to another person in such a way that it seems that the email was sent by someone else. It has become so common that we can no longer take for granted that the email one is receiving is truly from the person identified as the sender (Mali 2011). Acc. to CCVC report 2010, 41.7% have received hate messages from various persons and 45.5% have been targeted because of her sexuality or feminine ideologies. Only 8.3% prefer to report to Police which was very less (Halder and Jaishankar 2010: 18).
- **Cyber Pornography:**
- According to A.P. Mali, "It is the graphic, sexually explicit subordination of women through pictures or words that also includes pornography is verbal or pictorial material which represents or describes sexual behavior that is degrading or abusive to one or more of participants in such a way as to endorse the degradation. The person has chosen or consented to be harmed, abused, subjected to coercion does not alter the degrading character of such behavior" (Mali 2011).
- **Cyber Morphing:** This crime is related with pornography and we can also say it, a cyber obscenity. Female members' photographs are taken from their personal albums and are morphed for pornographic purpose by using parts of the pictures, for example, the head and up to breast (HalDer and JaishanKar 2009: 12).

- **Cyber Harassment via Emails:** It includes bullying, blackmailing, threatening or cheating etc. via email. E-harassment is similar to the letter harassment or felony, but creates problem quite often when it is posted from fake ids or cloned profiles etc. with the intent to terrify, intimidate, threaten, bother, harass, humiliate, or denigrate to female netizens (Agarwal 2013).
- **Cyber Hacking:** In this kind of cyber violence, some particular targets are chosen for hacking their profiles, using their personal information for evil purposes. Moreover, the hacker may even distribute open invitations for having sex with the profile owner at her home address (HalDer and JaishanKar 2009.
- **Virtual Rape via Cyberspace:** This is another violent and brutal type of cyber victimization where women are targeted by the scoundrels or harassers in the cyber space. He either posts vulgar messages such as, “I will rape you”, “I will tear you up”, your internet id well be f..ed off” etc, or particular community members may “mob attack” the targeted female with such words which successfully creates more enthusiasm among other unrelated members to comment on the victim’s sexuality. Then the profile owner becomes a hot topic vulgar name calling, erotic discussions, sexual image etc (HalDer and JaishanKar 2009

Some suggestions and steps to tackle cyber crimes

We should take some steps to tackle this problem. Here are some steps and suggestions:

- **Change passwords time to time:** In fact, we all love to have easy-to-remember passwords because, it is simpler. If one wants to lower internet crime risk, changing password is a great way to make personal data and social networks safe and difficult to access for cyber criminal (Pennelli 2012).
- **Avoid revealing home address:** This is the rule for women in particular who business professionals are and very visible. They can use work address or a rent private mailbox. Thus, it can help them out in avoiding cyber stalkers (Moore 2009).
- **Maintain stable social relationships:** It is also the fact that we all like to believe that we should have 2000 friends. Dunban’s number7 suggests a limit to the number of people, a human being can have a proper social relationship with, and that number is 150. Probably, we don’t need those 2000 facebook friends, because we are likely physical unable to really know more than 150 of them. Maintaining a limit on the number of the people will ensure our information is distributed to people who you really know and away from friends-of-friends-of-friends who you actually do not know all too well (Pennelli 2012).
- **Awareness campaign against cyber crimes:** Awareness campaign must be set up from the grass root level such as schools, collages etc about cyber crimes like stalking cheatings, economic cheatings, defamatory

activities, misusing emails and social networking websites, virtual rapes, cyber pornography, email spoofing etc (Halder and Jaishankar 2010:

- **Seminars and workshops for better understanding of cyber victimization:** Police, Lawyers, social workers, and NGOs must be invited to education institutes, clubs, corporate offices, awareness-campaigns, seminars and workshops to discuss about legalities and illegalities of cyber conduct among adults inclusive of both genders. Reporting of cyber victimization at all levels directly to the police and NGOs working cyber crimes must be encouraged. Secondly, workshops and seminars must be conducted for the police personnel for better understanding of such kinds of victimization and quick responses towards the complaints. Academic and legal experts, NGOs etc. must be invited for such workshops and seminars (Halder and Jaishankar 2010.
- **Rigid and stringent laws:** India must bring in more rigid and stringent laws for cyber crimes against women in the cyber space. It is evident that present India's Information Technology Act includes only few sections for cyber crime, especially against women, hence to curb cyber crimes, either IT Act must be re-modified or a separate law on cyber crimes should be created (Halder and Jaishankar 2010: 22). Proper law and order against crimes may lead to create good society.
- **Use common sense**: Despite the warnings, cybercrime is increasing, fueled by common mistakes people make such as responding to spam and downloading attachments from people they don't know. So, use common sense whenever you're on the Internet. Never post personal information online or share sensitive information such as your social security number and credit card number. Exercise caution when clicking on any links or downloading any programs.
- **Be suspicious**: Even if you consider yourself cyber savvy, you still need to keep your guard up for any new tricks and be proactive about your safety. Backup your data regularly in case anything goes wrong, and monitor your accounts and credit reports to make sure that a hacker has not stolen your information or identity. Although protecting yourself does take some effort, remember that there are a lot of resources and tools to help you. And by adopting a few precautions and best practices, you can help keep cybercrime from growing. McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. All rights reserved.

Conclusion

It concludes that the visibility to overcome the cyber crimes against women as a whole is challenging and the only way is to understand cyber crimes. Government needs to strengthen the legal system to lower cyber crimes, because criminals consider it much easier than traditional crimes due to less chance of being caught and fewer penalties

References

Agarwal, Rohit. CYBER CRIME AGAINST WOMEN AND REGULATIONS IN INDIA. 2013. Available at: <http://www.tmu.ac.in/gallery/viewpointsdcip2013/pdf/track4/t-403.pdf>.

Ahmad Shawal A. 2012. Facebook, Manfaat atau Mudharat. In. Melati Sabtu (Ed,), Penulisan Ilmiah Kolej Komuniti Temerloh. Temerloh: UPeN, KKTM.

Anita A. R. dan Nazura A. M. 2004. Jenayah Berkaitan Dengan Komputer Perspektif Undang-Undang Malaysia. Kuala Lumpur: Dewan Bahasa dan Pustaka.

Duggal ,Pavan(2009).Cyberlaw:The Indian Perspective, New Delhi: Saakshar Law Publications.

Ghosh, Sumit (2010). Cyber crimes: A Multidisciplinary Analysis,New york:Springer Publications.

Halder, Debarati and K. Jaishankar. CYBER VICTIMIZATION IN INDIA. A Baseline Survey Report. Tamil Nadu: Centre for Cyber Victim Counselling, 2010: 1-22.Available at: http://www.cybervictims.org/CCVCresearchreport2010.pdf

HalDer, Debarati and Karuppannan JaishanKar. "Cyber Socializing and Victimization of Women." September 2009: 5-26. Available at: <http://www.doiserbia.nb.rs/img/doi/1450-6637/2009/1450-66370903005H.pdf>.

http://cirjah.com/ojs/index.php/JAH/article/download/85/pdf_30.

Jalaluddin A. M. 2008. Siber Urbanisme: Pemikiran Melayu Tentang Bandar Pintar. Sari, (26), 111-125.

Jameson ,Fredric(2003). Postmodernism, or, The cultural logic of late capitalism,USA:Duke University Press

Jewkes ,Yvonne(2006).Crime Online, Canada: William Publishing.

Mali, Adv. Prashant. IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1. December2011.Availableat:<http://www.csiindia.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b 4b434c5919b6&groupId=10157>.

Moore, Alexis A. 12 Tips to Protect Yourself From Cyberstalking. 8 January 2009.Available at: <http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm>.

McQuade,C.Samuel(2008).Understanding and Managing cybercrime,Boston:Allyn and Bacon.

Pennelli, Paul. Cyberstalking Awareness: Protect Yourself On-Campus and Beyond With These 7 Steps. 31 January 2012. Available at: <http://blog.gradguard.com/2012/01/cyberstalking-awareness-protect-yourself-on-campus-and-beyond-with-these-7-steps/>.

Rusli H. A. et al. 2003. Teknologi Maklumat dan Penggunaannya. Petaling Jaya: Prentice Hall Pearson Malaysia Sdn. Bhd.

Termimi, M. A. A., Rosele, M. I., Meerangani, K. A., Marinsah, S. A., & Ramli, M. A. (2015).

Women’s Involvement in Cybercrime: A Premilinary Study.JOURNAL OF ADVANCES IN HUMANITIES, 3(3), 266-270.

Wall, David (2004).Cybercrimes and Internet,New York: Barnes & Noble.

www.dell.com/…/top_10_steps_to_protect_against_cybercrime_dell_en.