Sindhuniv. Res. Jour. (Sci. Ser.) Vol. 51 (01) 25-30 (2019)

http://doi.org/10.26692/sujo/2019.01.06

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Study of the Governing issues for Implementation of Cyber Security system and Digital Morals in Pakistan

A. B. BROHI, P. K BUTT[++], S. S. SHEIKH. A. MAHER, F. NAVEEN, H. A. MAHESAR*

Information Technology Centre, Sindh Agriculture University Tandojam, Pakistan

Received 21st September 2018 and Revised 16th December 2018

Abstract: The scenario of cyber oppression inPakistan needs to be studied in detail is ironic, even though cyber victimization includes abuse of fundamental rights and gender harassments, hardly any solid step has been taken to curb this. Most ISPs and networking sites adhere to what we call cyber-crimes and cyber rules and regulations which may give rise to opportunities to experiment with personal freedom, especially freedom of speech and expression and right to privacy. In Pakistan, some of such cyber-crimes may give rise to abuse of fundamental rights guaranteed by our constitution. In Pakistan, matured adults who are internet users must understand that what is offensive in the real space, must be maintained as offensive in the cyber space also. Cyber network has opened the gateway to a global village which may form its own rules and ethics but that in no way should encourage abuse of personal rights and freedom.

Keywords: Cyber-crimes, e-governing, wireless network, hacking, digital world, privacy, cyber rules

1. INTRODUCTION

At present, here is no decided upon universal definition of what founds cybercrime. As noted by Chang (2012) (Muhammad *et al.*, 2014) terms such as "cybercrime", "cyber-crime", "computer crime", "computer-related crime", "hi-tech" crime," "technology-enabled crime", "e-crime", and "cyberspace crime" are often used interchangeably. The meaning of cybercrime is broad and may be better understood as an umbrella term encompassing a variety of activities. For example, online child exploitation, state sponsored hacking and theft of hardware is sometimes grouped under cybercrime. Such crime can also be classified based on whether a computer is an instrument, target or merely incidental to a crime (Arpana and Meenal, 2012). The huge development of data engineering and information technology has suddenly changed the world. It has brought about the separations to shrink and digital data over the globe as it happens. In the meantime, it additionally offers help to vulnerabilities, dangers, cheats and criminal acts in the internet on cyber world. The straightforward entry, easy to understand hacking apparatuses and advancement in digital assets has encroached the security of the people, associations and states.

Pakistan is confronting multifaceted digital dangers in the present period. Trepidation of crime suggests perceived criminality earnestness, seen danger of victimization, and exploitation encounter as the three noteworthy prognosticators for anxiety of malefaction. In the present study, I test these components on digital cyber-crimes, as their associations with anxiety of digital crimes are by and large unexplored in the writing. Decisively, four digital computer-generated crimes are selected, including: online trick, digital harassing, advanced theft, and computer versus (Brohi and Kamran.2012). Adolescents today are familiar with a technology enabled world where they can connect with others through online communication and information technology, texting on their phones, chatting by Skype, and video messaging (Debarati, and . Jaishankar, 2010), Pakistan has no selective enactment committed for data engineering contrasted. It is disturbing that because of unfamiliarity, rate of E-exploitation is expanding. E-Victimization is the sort of exploitation that does not happen eye to eye. It happens through online computer technologies or other electronic gadgets or programming.

2. KEYS:

1. The level of awareness of cyber crimes
2. Frequency in cyber networking
3. Knowledge of victimization
4. The incidents of victimization occurred, and security measures adopted
5. Hacking/stalking/phishing
6. Victimization through Cyber Friends
7. Police and legislation available
8. Awareness towards legal rights

3. AIM OF THIS RESEARCH

In Pakistan, cybercrime and exploitation in the internet had remained a subject of extraordinary fear,

[++]Corresponding author: Pinial Khan Email: pinial@yahoo.com

*University of Sindh, Jamshoro, Pakistan

however needs mindfulness. Strange blend of nature of assaults constantly changing patterns of the exploitation, constrained information about immediate laws, which address cybercrimes in Pakistan and privileges of exploited people in instances of digital assaults, help enormously towards shaping an irregular methodology to digital exploitation situation. There are a great many web clients in thought now who are frequenting the internet all the time for expert, business, standardizing and education purposes. In this research, we will choose a case study of Pakistan for awareness of cyber-crimes and its prevention for victimization.

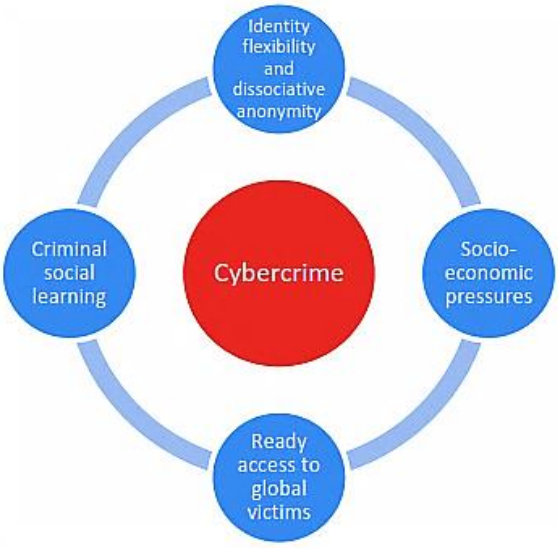

Fig: 1.1 Factors links to increases in cybercrime

Digital harassing exploitation encounters are emphatically connected with alarm of exploitation, and apprehension of online exploitation are discovered to be associated with saw hazard in a study concerning school understudies' utilization of Facebook

3.1-TYPES OF CYBERCRIME

3.1.1-Hacking: To hack is to gain unauthorized access to a computer that does not belong to you. In today's modern world, this is a grave problem and it is extremely important to find a solution to minimize its consequences. Howard Raffa, influential Bayesian decision theorist and pioneer in the field of decision analysis, has given a guidance to the solution of this problem in these words.

"Game theory, however, deals only with the way in which ultra-smart, all knowing people should behave in competitive situations, and has little to say to Mr. X as he confronts the morass of his problem."

3.1.2-Insiders: According to a research, insiders pose greater threat than outsiders, accounting for 65% of the nuisance. There could be multiple reasons why a staff member or a colleague would be interested in stealing your data.

3.1.3-Outsiders: The outsiders for an organization are not a part of the organization and do not have legitimate access to the company's machines. The outsiders for an individual can be anyone who is not given access to the device by the owner but tries to get illegitimate access. In this section, we will try to focus on the hacking of wireless networking by outsiders who are not given a password to the network. We will also discuss how firewall as a protection mechanism may fail and why from outsiders.

3.1. 4-Wireless Networking: When LAN and WAN cables were used to connect to the network, the network operators has control over who uses the network, but with the advancement in technology anyone with the Wi-Fi password can connect to the network. Wi-Fi has gained popularity as it cuts down on cable costs and provides the convenience of being used on any portable device and does not require a huge desk space. However, Wi-Fi has attracted hackers who either want free connectivity or have other motives such as stealing data. Locating the unprotected Wi-Fi is extremely easy for a hacker as any device with wireless connectivity will display the available networks and give the option of connecting to any of them.

3.1.5-Firewall: Firewall is a very important tool for security from outsiders. A firewall is an electronic filter that allows you to block communications over the internet according to their source, destination, direction or port number. Note that the firewall only protects from the outsiders, not from the insiders. Firewalls need to be configured properly or the hackers can use techniques such as tunneling which allows the internet traffic to be send over non-standard ports to confuse and bypass the firewall. Thus, one needs to be careful when selecting a firewall for personal or business use. This can be done by doing research and survey of the options you are considering. Please note that companies that offer firewall and security use hacking competitions' success stories to market themselves by boasting that the firewall stood up to millions of attempted attacks.

3.1.6-Denial of Service Attacks (DoS): Denial of service attacks require the hacker to use the publicly available facilities of the target computer and make the network or the computer temporary unavailable to its legitimate users. The hacker does not need to worry about overcoming security barriers such as passwords and firewalls. There is a limit to the number of requests the server can process per minute and denial of service attacks exceed the limit to the extent where the system can no longer process the requests resulting in a system crash. Committing such attacks is easy as it only

involves selecting proper tools and a target. Previously, the Denial of Service Attack's traffic originated from a single source and the solution would be to somehow manage to make your machines work and block the IP of the source that is attacking you. This also required the attack source to have a larger server than the victim to be able to send the enough volume of data. However, the attackers progressed and came up with the Distributed Denial of Service (DDoS) Attacks mechanism.

4. RESEARCH METHODOLOGY

This research study would be based on surveys and conducted cyber security at located in Pakistan.

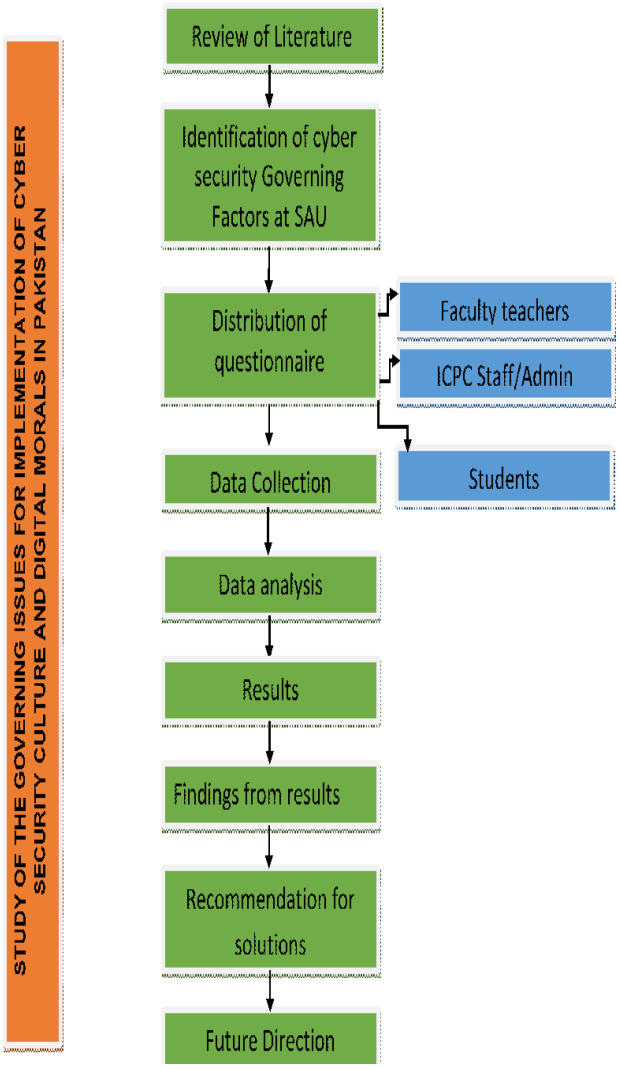

Fig: 2.1 Cyber Security Rule in Pakistan

4.1-SOLUTIONS: There can be many solutions to limit the threat from both outsiders and insiders and the perfect one would vary from one organization to another. Protecting oneself can be as easy and cheap as hiding the name of a website and it can be as expensive as outsourcing the responsibility to someone else. Security through Obscurity (STO) is the belief that a system of any sort can be secure if nobody except the owner is allowed to find out anything about its internal mechanisms which reduces the need for additional security. Example can be using an obscure URL instead of a very difficult password. Since nobody except the owner would know of the existence of the domain, nobody would try to hack it which reduces the need for a password to be extremely strong. Since the existence of the protected system is itself a secret, it does not require further security. The disadvantage of using such a technique is that anyone with the URL can breach and the owner might not even notice any defacement. Thus, STO should be used as a layer, but should not be relied on solely for protection. If a company that does not have the resources to take care of their IT security, one option is to outsource the task to Managed Security Service Providers (MSSP). They can do simple routine work such as resetting forgotten passwords, installing patches on servers as well as mundane tasks like checking firewall logs for evidence of attempted hacks while keeping a watch-eye for alerts from Intrusion Detection Systems. They perform regular analysis on the firewall logs and work to investigate any entry that arouses their suspicion. However, they would require administrator level passwords to do their job properly, which transfers the risk of Insiders from one premise to another. This might be riskier in the sense that one doesn't know the MSSP company employees personally. But as we have learned, the insider problem cannot be eliminated, it can only be minimized, and in this case, we can do that by signing a legal contract with the company and only outsourcing the important functions and not all. When deciding the MSSP Company, you should do a research and ask the clients the company had had for feedback. You should make sure that the MSSP you choose has a 24 hour a day availability for all the days of the year including public holidays, so you get the rapid response you need. A satisfactory contract and SLA (Service Level Agreement) between you and the MSSP is vital so you know what kind of service and response times you can expect. Once the contract is made, it is recommended that you ask someone to try to hack the system just to make sure the company is meeting your expectations.

5. RESULT

5.1-AWARENESS OF (CYBER SYSTEM)

Table 3.1 Awareness among Cyber System

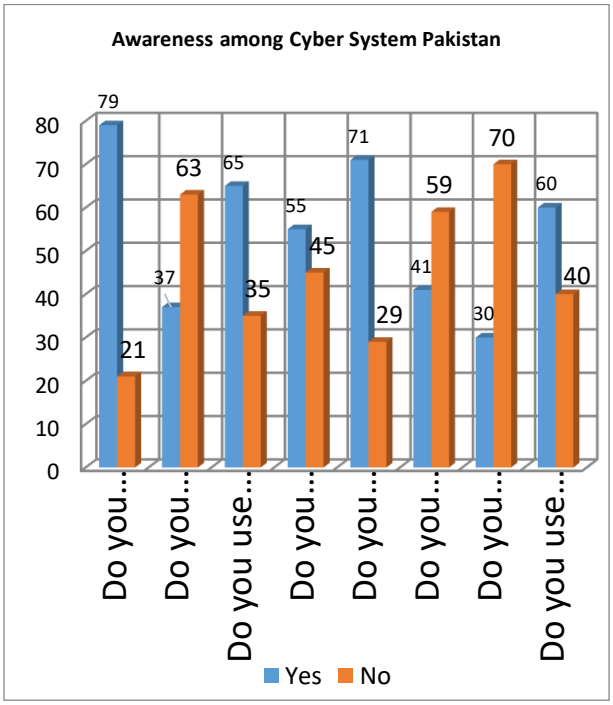

Fig. 3.1Awareness among Cyber System

Analyses: **(Fig. 3.1)** is showing the respondents awareness regarding Cyber-crimes. The (Cyber-crimes) could be well-defined in methodological term that, 1. The identified the minimum age, that is required for entrance in cyber community, 2. In what way to use their right "(Freedom of Speech)", 3. Activities that are involved with personal information sharing.

5.1.1-Minimum Age: The outcome is demonstrating that 79% respondents know with respect to least age that is fundamental to join digital network site and so on. While 21% respondents don't know with respect to least age to join the internet.

5.1.2Allow Other to Use Personal ID: Every one of the respondents are understudy of college and it is extremely disturbing that 37% respondents answered that they permit others (Friends) to utilize their own ID and secret key, when we see that 79% respondents realize the base age to join the internet on other hand 37% respondents enable their companions and relatives to utilize their own id and secret key to talk with others or mail them.

5.1.3Safety Measurements: The 65% respondents know with respect to security measures or self-assurance apparatuses. It is possible that they know it after any occurrence, companion or through accessible web material. The respondents utilize web separating, square upsetting individual, bolted individual dividers, collections or companion records and so on. While 35% respondents don't know with respect to these strategies or they don't care to utilize.

5.1.4Mail Back: The 55% respondents answered that they are utilized to mail back to obscure individual while 45% respondents said that they don't care to answer on mail of obscure sender.

5.1.5Share Personal Information: The 71% respondents are utilized to share unique data moreover contact numbers, age, locations or individual emotions. They share their own data with which they have never found in genuine world or they know just on the internet. While 29% respondents share their own data with just known people.

5.1.6-Free Speech: 41% respondents feel that there must be control on free discourse. These respondents have a place with Pakistan and they are utilized to utilize visit rooms or other long range informal communication destinations like Facebook, Orkut and Instagram. These destinations are being worked by US law of "(Freedom of Speech) while in Pakistan, the significance of (Freedom of Speech) is extraordinary. Article 19 of constitution of Pakistan 1973 portrays it as "Each national will have the privilege to the right to speak freely and articulation, and there will be opportunity of the press, subject to any sensible confinements forced by law in light of a legitimate concern for the brilliance of Islam or the respectability, security or protection of Pakistan or any part thereof, agreeable relations with outside States, open request, tolerability or ethical quality, or in connection to disdain of court, 1 [commission of] or affectation to an offense (Freedom of Speech, 1973). The idea of (Freedom of Speech) under US law is "Congress will make no law regarding a foundation of religion, or forbidding the free exercise thereof, or condensing the (Freedom of Speech) or of the press, or the privilege of the general population quietly to collect, and to request of the administration for a review of complaints (first Amendment)."59% respondents trust that there is neither need to control on (Freedom of Speech) nor alterations.

5.1.7 Reading Policy Guidelines: The strategy rules of different digital networks are critical source to create (Cyber-crimes). The vast majority of informal communication locales utilize their own approach rules to create it. The point of these rules to keep their clients from, hacking and its related issues, e-violations, sexual wrongdoings, kid misuse and erotic entertainment. At some point these networks don't put stock in to ensure religious considerations.

5.1.8Nick Names: 60%respondents concede that they utilize Nick (Pseudo) names on the internet. A pseudo name, that a man or gathering use for explicit reason and it is diverse frame his/her genuine name (Pseudonym, 2013). Along these lines, the significance to utilize these names might be to ensure their personality. 40% respondents don't utilize monikers.
Under this part we will study the frequency level of respondents towards online activities.

Table 4.1 Frequency in cyber networking

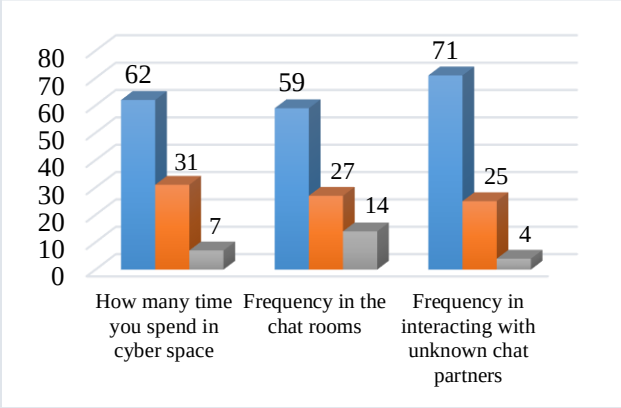

Fig: 4.1 Frequency in cyber networking

The **(Fig. 4.1)** is showing that 62% respondents are highly active on internet. They use more than 06 hours on various chatting networking sites. 31% respondents spend 03-05 hours and 7% respondents spend below than 02 hours on chatting networking sites. The greater part of the respondents is having a place with high and moderate classification. 59% respondents are exceptionally dynamic in visit rooms, 71% respondents are on high danger of exploitation because of connection with obscure people in digital networks and 27% respondents put in 03-05 hours and 14% least 02 hours every day in talk rooms.

Government Department in Pakistan: Results of study demonstrate that mindfulness with respect to government division to control digital violations is extremely poor. Just 32% respondents realize that an administration office is attempting to control digital violations, 48% respondents trust that digital wrongdoing control division don't exist, and 20% respondents don't know either office exist or not.

6. CONCLUSION

The scenario of cyber victimization in Pakistan Country looked-for to be premeditated in detail is ironic that even though cyber victimization includes manipulation of fundamental rights and gender harassments, hardly any solid step has been taken to curb it. The most ISPs and chatting sites observe to we seen cyber-crimes and cyber rules and regulations which may give rise to opportunities to experiment with the personal freedoms, especially freedom of speech and expression and right to privacy. In the Pakistan connecting people sites value system, some of such cyber-crimes may give rise to several abuses of fundamental rights guaranteed by our constitution. Matured Pakistani internet users must understand that what is offensive in the real space, must be maintained as of offensive in the cyber space also. The Cyber entertaining has opened the gateway to a global village which may form its own rules and ethics but that inno way should encourage abuse of personal rights and self-determination.

REFERENCES:

Arpana and C. Meenal, (2012), Preventing cybercrime: A study regarding awareness of cybercrimein Tricity. International Journal of Enterprise Computing and Business Systems, 2(1).

Brohi M. N. and R. Kamran.(2012)"Scientific Awareness about the Computer Forensic to Face the E-Criminal Activities of the E-User", International Journal of Computer Applications (IJCA) 2012, Vol.49- No 4, Year of Publication: 2012. Published by Foundation of Computer Science, New York, USA.
http://www.ijcaonline.org/archives/volume49/number4/7618-0668.

Debarati, H. and K. Jaishankar, (2010), Cyber victimization in India: A baseline survey report Tirunelveli India: Centre for Cyber Victim Counseling.

Holtfreter, T. C. and K. Reisig (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3): 267-296.

Hinduja, S. and J. Patchin, (2008). Cyber bullying: An exploratory analysis of factors related to Offending and Victimization. Deviant Behavior, 29,129-156.

Kunz, M. and P. Wilson, (2004). Computer crime and computer fraud. Professional Master's Degree Thesis. Department of Criminology and Criminal Justice in University

Muhammad G., N. Allah and A. Robina, (2014), Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries. Journal of Information Engineering and Applications. ISSN 2225-0506 (online) Vol.4, No.4. of Maryland.