Causes and Consequences of Cybercrimes:
An Exploratory Study of Pakistan

Adnan Riaz
Department of Business Administration
Allama Iqbal Open University
Islamabad, Pakistan
adnanriaz.aiou@gmail.com

Adeel Riaz
ECCO Office
Islamabad, Pakistan
adeel.pakchina@gmail.com

Abstract— **Countries across the world are deeply concerned about the cybercrimes. Experts and practitioners always emphasize on collaborative efforts to investigate and control illegal activities in virtual environment. Countries differ significantly on socio-economic continuum. Due to cultural dissimilarities, criminal activities as well as their causes and consequences also vary from region to region. This study was an effort to identify contextual factors stimulating illegitimate activities in cyber environment and to suggest remedial measures in this regard. With the help of focus group sessions comprising ten participants from diverse background, a discussion was held to explore the causes and consequences of cybercrimes. The consolidated results are presented duly agreed by the panelists.**

Keywords — Focus Group, Person-Job-Fit, Educational Surveillance

I. INTRODUCTION

Information technology (IT) has substantial impact on all spheres of life. Mobiles, tablet-apps, laptops, telecommunication media and many other gadgets and devices have accelerated the pace to communicate and exchange information. The developments which couldn't have been imagined to take place in decades, are now possible within few years. The world is called a global village because of communication ease provided through information technology. Broadly considering the sectors like banking, education, mass media, business, tourism, nearly all are the beneficiaries of digital age. However, the facilitation provided can't be examined in isolation. Despite advantageous nature of IT, it has also brought challenges which needs attention at both micro and macro levels. Among key challenges, cybercrimes have acquired the attention of policy makers across the globe. Cybercrime is the term used to refer to the crime rendered in the virtual environment. It describes the crimes emerging by mean of interconnected technologies [18]. There is no doubt about the direct costs, indirect costs and defense costs, which a country has to bear as a result of cybercrimes [2]. A wide spread belief about cybercrime characterizes developed countries as more vulnerable to cybercrimes [6]. However, developing countries are also experiencing the cybercrimes with the same frequency as the rest of the world. Citizens belonging to developing world can easily be betrayed due to the lack of educational facility and awareness.

Considering the example of Pakistan, it is a country with diverse potential. Pakistan is normally conceived as agri-based economy [16]. But it has many key features which can help to bring categorical growth. The strategic location of Pakistan [12], unexplored natural resources [7;15], potential tourism sites [8;9;11] and shipping port [7;15] can certainly accelerate economical growth. Nevertheless, the best manpower can also be a cornerstone in the development [10]. Despite some other reasons, Pakistan has always been a victim of corruption and malpractices [4;12]. The culture of malpractices has also been duly penetrated in the cyber environment.

Table-I
Recoveries made in Different Cyber Crime Cases by National Response Centre for Cyber Crimes

Title of the Case	Amount Recovered In Millions
Fraud Case of Meezan Bank	35
ATM Fraud case of Allied Bank of Pakistan	7.4
Altering of balance transfer system	4
Illegal transfer of money	3.9
National Bank of Pakistan ATM Fraud	2.5
Online website fraud	1.2
Total	**54**

Source: http://www.sja.gos.pk/Events/Cyber Laws Workshop

To deal and address the issues of cybercrimes, the government of Pakistan established the National Response Center for Cyber Crimes (NR3C) under Federal Investigation Agency. The missions of NR3C are manifold. In addition to provide security education and trainings to government and private organizations, it is actively engaged to detect and redress the frauds, malpractices and financial embezzlements taken place in virtual environment. Pursuing its mission, NR3C has liaison with different international agencies to cooperate and make joint efforts in this regard. Because fighting against cybercrime requires holistic approach being concern of all societies [1]. Table-I presents some achievements of NR3C.

978-1-4799-7620-1/15/$31.00 ©2015 IEEE

II. Methodology

A. Subjects/Sample

The study endeavored to know the contextual causes and consequences of cybercrimes in the local environment of Pakistan. Since the developing world is attributed with different characteristics therefore, this study was among few which were initiated to know the reasons behind cybercrimes in Pakistan. A panel of expert was invited to discuss the issue in order to come at reasonable conclusion. An attempt was made to invite and constitute a diverse panel of experts. For that, experts were invited from different walks of life. The composition of the group is given in the table-II.

Table-II

S. No.	Focus Group Member	Qty	Reason
1	elearning Coordinators	2	Association with online learning
2	Professional (GM of Private Organizations)	1	Coordinating Online Transaction of Co.
3	Ex-Official	1	Experience of Handling Cybercrime Cases
4	Teachers / Educators	2	Coordinating IT/Cyber Courses
5	IT Expert	1	Practitioner
6	Entrepreneur	1	Net Club Owner
7	Students (Graduating and Graduated)	2	Studying Information Systems and Active Users
	Total	10	

The group members had any kind of association with cyber environment. The heterogeneity among the subjects increased the likelihood of greater interaction and diverse views about the topic under consideration. However, the subjects lacked any association (except at serial # 1) which could result to exchange views before meeting.

B. Instrument

Focus Group discussion was held to figure out the reasons behind cybercrimes and outcomes. The focus group is a research strategy for understanding complex issues. Normally, focus groups are used for exploratory studies, since this study pertained to identify the contextual factors therefore, focus groups deemed appropriate for the purpose. Focus groups help to explore a particular topic in detail by providing in-depth insight by group participants who are normally experts in their respective areas. The group members put forward their own views, challenge the others' with arguments and help to refine understanding with debate [3].

Experts from different areas were selected and invited for the discussion. All the participants were given detailed orientation about the topic under study. This enabled them to come well prepared. The day and time were also communicated through the registered postal service and supplemented through text messages. Participants were also informed about the confidentiality measures taken in this regard by highlighting sole academic purpose of the study and the participations of the individuals were voluntary. It was further ensured that the results and names of the participant would not be disclosed without their permission.

Each of the group participants was given adequate time to explain their understanding about the causes and consequences of cybercrimes. They could support the argument with personal experience, observation or any other evidences. The researcher controlled the discussion as moderator. Two of the volunteers were assigned the task to jot down the proceedings. All the participants showed due respect to the understanding of other participants and helped to come at consensual conclusion.

The complete session was twofold. After tea break, the next session was held to discuss the remedies/solutions to cope with this menace. This session was equally important as the implications of the study were supposed to be highlighted. Ample time was allocated and group participants showed some consensus in this regard.

III. Results

Causes and Consequences of Cybercrimes

A. Education and Awareness;

The calculated illiteracy rate of Pakistan falls 79% whereas Pakistan ranked at 180 among 221 countries about education. The prevailing illiteracy deems impetus of many problems and cybercrime is one of them. Specifically speaking, users with inadequate internet experience are more vulnerable to cybercrimes being naïve and excited. They can be easily deceived and maneuvered. Normally such users fall victim of financial frauds, computer trespassing, spam mails, information espionage, business forgery and many more.

Beginners in virtual environment have different fascinations. Offenders normally exploit the needs of the victims like educational, money, product, visa, medical cure etc. because of dearth opportunity to promptly verify the source. They are easily hunted and exploited.

B. Unemployment;

Unemployment rate in Pakistan is calculated as 6% in 2012-13 [5] which is quite high in comparison to any developed country. Even Pakistan relatively falls behind to other competing countries under developing arena. Internet becomes a vibrant source to search jobs or earn money in the contemporary environment.

The unemployment may cause problems at both ends. It may stimulate few users to exercise illegitimate tactics to generate income in shortest possible time. On the other side, unemployed individuals may resort fake and fraudulent websites and mediums for better employment opportunity. Though employed persons are also vulnerable to deceptive practices of the source. But unemployed persons are commonly tricked due to desperation caused by the circumstances.

C. Security and Safety Measures of the Organization;

Some of the cybercrimes are committed due to lack of security and safety measures taken from the organizations

concerned. It may be due to the fact that some organizations never have pro-active measures. Organizations lacking update security walls, antivirus and spam filters usually face issues like website hack, password loss, email spoofing, information theft, virus/worms attack, data diddling etc.

Some of the small and medium enterprises have limited funds available to protect their database when connected with internet. Funds shortage restricts their ability to either purchase latest and comprehensive security packages or to update the existing installations.

D. Culture and Personality;

Personalities also count a lot in the cyber environment. Some of the personalities are cynic in nature and can easily commit cyber crimes without feeling any remorse. Personalities take shape by the connectedness with the group individuals spend time. Society, school and parental care play a dominant role in the grooming of one's personality. In short there is always a pervasive role of culture in shaping the personality. In a myopic culture, individuals may have build-in negative affectivity. They accept many negative realities of life which ought to be discouraged from different quarters. When such individuals start taking part in the virtual activities, it provides them a safe place to play their cards. They can go to any limit with the assumption of enjoying invisible state.

E. Educational Surveillance

Due to the advent of technology as well as the ease of access to informational sources. Some databases, books, articles and other open sources, explain about the development of malicious software or other hazardous programme which may harm other system. Basically, such information sources are intended to educate students and available for learning purposes only, but this may lead towards another critical problem. For example, if a student is acquainted the knowledge about "How viruses are developed" may entice him/her to put other people in danger by producing and transferring viruses to others computers, if fall aggrieved for any reason.

A common example exists of those well versed with graphical and image editing software, can easily edit the images of others. Principally, the use of such software needs to be in productive way.

F. Person-Job-Fit

Law enforcement agencies have chronic problems of incompetent manpower. Though transparency remains a concern and highlighted by various quarters about government organizations, but the high performing organizations are more vulnerable if incompetent human resource is inducted. A proactive safety measures can only be taken, if competent inductions are made and updated after regular interval.

G. Resources and Equipment

A key concern was raised by one of the member associated with academia. Some of the institutes lack necessary resources to detect plagiarism which may cause piracy and plagiarism issues. Intellectual property rights, authorships, patents can only be protected if necessary resources and equipments are provided. Higher education commission has made tremendous progress in this regard, however such provision is not available in some universities even if it is provided, the concerned coordinators are not well conversant with its effective use.

H. Government to Government Cooperation

A desperate need exists between government to government cooperation to spot offender involved in cybercrimes. Notwithstanding, the laws are established, enacted, reviewed and updated on regular basis in developed countries but underdeveloped and developing countries fall behind in this regard. Precisely, a gap exists between different countries to realize the sensitivity of cyber issues. In some of the developing countries, cyber exploitations are not taken a serious concern like crimes committed in the real environment. Due to recent terrorism upshots which were not possible without information transfer through cyber means, some of the developed countries made strong liaison with other countries especially with Pakistan. The development is encouraging to address the terrorism and like issues but the cybercrimes are common features of nearly every discipline like marketing, journalism / mass media, banking and finance, e-government etc. Government to government cooperation is indispensible nearly for every field.

I. Competition

Due to stiff competition under the marketing and sales environment. Organizations have to wait and develop their goodwill for lasting relationships with their clients. Now most of the organizations are facing competition on account of their marketing strategies especially in case of undifferentiated products. Impatient organizations, start involving in unfair practices by means of advertising and sale tactics. Since developing countries have week rules and procedures to locate and trail culprits, may result various unhealthy practices in different environments from developing world.

J. Silent Vengeance

Relationships, social identify and outrage are also a key motivator to involve in cybercrimes. It has been observed among some of the students, the main impetus behind cyber defamation is relationship break-ups, grievances, misunderstandings or like reasons. Cyber world is perceived as a safe platform to retaliate and take revenge for any distasteful happenings in the real world. Such practices are even more common with the aggrieved individuals who can't retaliate in the real world.

IV. SOLUTIONS / RECOMMENDATIONS

After detailed deliberation, the panel put forward various recommendations. After consolidation, we may recommend the followings;

- Safety and security measures of the organizations should not be comprised. The government may craft strict rules and regulations about establishing safety

walls for the organizations highly vulnerable to cyber victims. This may help to a large extent if the safety and security is deeply ensured.

- Access to quality education is the fundamental right of every citizen. Educated society is comparatively less susceptible to cybercrimes. Therefore, governments need to allocate substantial budget for education. Computer literacy may be inculcated at very basic level. Computer ethics, business ethics, society ethics and like courses may be treated as a compulsory component of scheme of studies. Nevertheless education plays a dominant role in shaping personalities and transforming responsible generation.
- Since cybercrime is affecting every country across the world. There should be some joint efforts to cope with it. The efforts of United Nations (UN) and ITU are specifically encouraging. By strengthening and proper capacity building of such agencies may augment the effects.
- Fake emails for monetary enticement, abusive selling websites, predator journals and other exploitive mediums should be properly given and highlighted at official responsible agencies. This would enable users to authenticate the legitimacy of information / documents received through any source.
- High performing jobs should not be compromised on account of nepotism/favoritism during hiring process. An incompetent employee in cyber profession may have many repercussions. Right person at right job should be the foremost criteria in such ambits.
- To refrain students from illegal activities, all the institutes should be provided plagiarism detecting services (turnitin, ithenticate etc) and train them for their effective use.
- Competent and trained manpower should be inducted in IT wings of the organizations to safeguard their information sources and databases. As well as regular training opportunities may also be provided with respect to environmental demands and contemporary issues.
- Education should be need based with respect to sectoral / industrial demand. The courses and their contents need to be carefully designed. For example, students if understanding the development of virus or malware, may further attempt to develop such bugs to counter any regret. If such kinds of subject matter are indispensible to discuss and study, such should be dealt under surveillance.
- It has been observed that students studying comprehensive ethical contents (business ethics, society ethics, marketing ethics) are normally have strong ethical values and concerns. This may abstain themselves to involve in unethical practices in virtual and real environment. Therefore, IT / cyber ethics should be a core course at different levels. Students across the board need to study the theory as well as involve in ethical dilemmas during course of study.
- At government level dearth laws and statutes were promulgated to warn individuals from any illegal practices during early days of IT development. But now laws are enacted and agencies are entrusted the responsibility to redress the aggrieved individuals faced any of the deception. But there still exist a need to revise laws and regulation in view of the changed conditions. Monitoring existing laws and their revision should be a permanent feature considering the dynamic nature of cyber environment.
- It has also been observed that media reporting is normally confined to wrong doings and mal-practices happening in the real environment. Very few evidences can be traced where criminals were highlighted on the media committing cyber offences. The trails of offenders should be properly publicized for public awareness. The deeds should accordingly be penalized and highlighted to let public know about the consequences of such offense [1].
- Especially, individuals committing cybercrimes should be highlighted in authentic media with large readership and/or viewership. This would disseminate a message to the society about the serious consequences had to bear in case of any wrong doing in cyber environment.
- Conclusively, the house was agreed to emphasize government to devise policies for economical developments. Miseries are the cause of many evils. When common man gets what he deserves and adequately earning for his necessities, may help to a large extent in coping cybercrimes and related maneuvering.

V. Conclusion

Cyber crime has emerged as the key challenge across the world. It may be apprehended that the reported cybercrimes may increase exponentially with the increase in the technological pace, if the due attention is not paid. The severity of the crimes in cyber environment may differ from

country to country. But the incidences can only be addressed by joining hands and entrusting strong commitments.

REFERENCES

[1] E.B. Ajala, (2007),Cybercafes, Cybercrime Detection and Prevention, Library Hi Tech News, 24 (7), 26 – 29.

[2] R., Anderson, C., Barton, R., Böhme, R., Clayton, M.J.G Eeten., M., Levi, T., Moore, and S., Savage, (2013), Measuring the Cost of Cybercrime, *The Economics of Information Security and Privacy*, 265-300.

[3] A., Bryman, and E. Bell, (2003), Business Research Methods, Oxford University Press, Oxford.

[4] W.D., Davis, and W.L. Gardner (2004), Perceptions of politics and organizational cynicism: An attribution and leader–member exchange perspective, The Leadership Quarterly , 15, 439–465.

[5] Employment Trends (2013), Government of Pakistan, Statistics Division, Pakistan Bureau of Statistics, Retrieved from http://www.pbs.gov.pk/publications

[6] M. Goodman, (2010), International Dimensions of Cybercrime, *Cybercrimes: A Multidisciplinary Analysis*, 311-339.

[7] A. Hassan, (2005), Pakistan's Gwadar Port – Prospects of Economic Revival, Naval Postgraduate School, California, USA.

[8] L.K. Richter, and W.L. Richter, (1985). Policy Choices in South Asian Tourism Development, Annals of Tourism Research, 12 (2), 201–217.

[9] L.K. Richter, (1999). After political turmoil: The lessons of rebuilding tourism in three Asian countries. Journal of Travel Research, 38, 41-45.

[10] A, Rahman, (2011, 05 April), Time to save the Higher Education Commission, Retrieved from http://tribune.com.pk/story/142945/time-to-save-the-higher-education-commission/

[11] G. Hancock, (1983), The Beauty of Pakistan, SAY Pub. Karachi, Pakistan.

[12] Islam, N. (2004). Sifarish, sycophants, power and collectivism: administrative culture in Pakistan. Int. Rev. Admin. Sci., 70(2): 311-330.

[13] G. Hofstede, (1991), Cultures and Organizations: Software of the Mind, London: McGraw-Hill Book Company.

[14] G. Hofstede, and M.H. Bond, (1984), Hofstede's Culture Dimensions: An Independent Validation Using Rokeach's Value Survey. Journal of Cross-Cultural Psychology, 15(4), 417-433.

[15] H.Y., Malik, (2012), Strategic Importance of Gwadar Port, Journal of Political Studies, 19(2), 57-69.

[16] A., Parikh, F., Ali, and M.K., Shah, (1995), Measurement of Economic Efficiency in Pakistani Agriculture, American Journal of Agricultural Economics,77(3), 675-685.

[17] A.S., Tsui, S.S., Nifadkar, & Y.A. Ou, 2007. Cross-national, cross-cultural organizational behavior research: Advances, gaps, and recommendations. *Journal of Management,* 33: 426-478.

[18] D.S. Wall, (2008) Cybercrime and the Culture of Fear, Information, Communication & Society, 11(6), 861-884.