Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.5, 2015

A Quantitative Approach to Cybercrimes Impact on Society in Pakistan
Case Study: Business Community of Southern Punjab

Naqvi Hamad[1*] Abdul Manan[2] Ghulam Shabiralyani[2] Nadeem Iqbal[3]
1.Policy and Strategic Planning Unit, Health Department Punjab, Lahore, Pakistan
2.National College of Business Administration & Economics Lahore, Campus D.G.Khan
3.Ghazi University D.G.Khan

Abstract
This paper describes the nature of cybercrime which occurs in Pakistan. Internet crimes in Pakistan are in the growing stage due to less knowledge of internet and facilities. The objective of this study is to give the awareness to the business community about the harmful impact of cybercrimes. Preventive measures are also discussed in this context. The targeted population for this study was the business community of major districts of the southern Punjab, Pakistan. Information was received through questionnaires and interviews. Data collected was obtained through likert scale questionnaires from target population. The response rate was 100%.The collected data was analyzed through SPSS software by using regression and correlational analysis. The finding shows that the business community is avoiding and feeling unsecure to deal business transactions through the internet due to the harmful impact of cybercrimes.
Keywords: cybercrime, types of cybercrimes, e-business.

1. Introduction

The internet is becoming popular day by day because of its some distinct sorts. Internet has brought a radical variation in socioeconomic and communication transaction. Society is facing advance kind of crimes that are known as cybercrimes after invention of computer. Cybercrime is dominant form of international crime that has been suffered by the worldwide revolution in ICTs (Barr & Pease, 1990). Cybercrime has become very common as well as very precarious crime in today's society. The number of committers of this crime is increasing day by day to use technology unlawfully for their own gain (Gjata 2007). The dangerous aspect of cybercrime is that the sufferer fails to acknowledge the cause of their ill-fated. Victims not only should report any kind of suspicion and/or crime, but also victim needs to point out the distrusted machine so that police can eliminate it in order to collect evidence from the machine's hard drive. Cybercrimes is a common matter of the current world. Cybercrime is a multifaceted crime and its sort is so massive.

Cybercrime covers a broad horizon of criminal activity by a computer. Some common illustrations of cybercrime contain financial scam, identity theft, cyber bullying and website destruction. At an organizational level, cybercrime is used for hacking of customer databases and theft of intellectual property. According to Council of Europe "Any criminal offense committed with the help of a computer network is identified as cybercrime" (Council of Europe Convention on Cybercrime 2001:8). Cybercrime is a criminal action in which computing devices or other forms of ICTs are used (Pati, 2003).There is no exact definition of cybercrime as different researchers and agencies gave different definitions according to their place and state. It has different name like computer crime, Internet crime and high-tech crime (Brenner and Goodman 2002:6, Kowalski 2002:7). There are many types of cybercrime existing in the present world. Researches and investigations show that throughout the world the kinds of crime have to explore yet; which occur generally in every place in the world. "Identity fraud" is a type (Blindell 2006). It is defined as identity fraud refers to the acquisition of money, services, goods or other welfares through the use of a false identity (ACPR 2006:14). The term 'Identity theft' in the United States of America is generally used to cover all types of identity crime. In United Kingdom it is known as identity fraud. In Australia, it involves the use of identity crime as a generic description (ACPR 2006: 5). Cyber fraud has a potential to widen the digital division, crush the information structure and affect consumer confidence in online transactions (Salifu, 2008; Longe et al., 2009; Oumarou, 2007). Cases of online fraud pertaining to credit card crimes, contractual crimes and advanced fee fraud have been fairly registered (Magele, 2005; Longe et al., 2009). Financial Fraud is another type of cybercrime (Fafinski 2008, Graycer 2000). It is clear as the use of fraud for direct or indirect Financial or material gain (Fafinski 2008). It comprises credit and debit card fraud, internet banking and money laundering (Graycer 2000, parliamentary committee on the Australian crime commission 2004). Cyber criminals capitalize on system unawareness liabilities and gullibility on the part of users to commit their shocking crimes. Between 2006 and 2007, financial damages caused by cybercrimes in the United States alone increased dramatically from $52.5 million in 2006 to $67 million in 2007 (Richardson, 2008).

Computer misuse means unauthorized access to a computer system such as simple hacking, serious

hacking and unlawful change of computer material such as viruses. A sexual offence is most alarming type of cybercrimes at present because of the accessibility of pornography (Fafinski 2008). We call it pornography which is offense against ethics as it contains child pornography and other offenses against minors, stalking, harassment, hate speech etc. (Brenner and Goodman 2002:10). This class of cybercrime covers a variety of conduct that has an objectively ascertainable sexual contents including pedophilic activity such as grooming a child for sexual activity. At present Spam, Botnets, Phishing are the matter of concern at Cyber world because it causes lots of harm of computer system and data management (Jaishankar, Pang and Hyde 2007). If users are unaware that their personal information is actively being targeted by criminals, they may lack the standpoint needed to identify phishing threats and may not take the proper defense when conducting online activities. Many factors affecting why customers are concerned about their online banking security. The same factors are also driving the need for enhanced authentication for online banking solutions. These factors include the growing number of phishing attacks, the increased usage of pharming and malware, and widespread data security breaches (Williamson and Gregory, 2006). Phishing is a relatively new type of identity fraud that refers to the act of trying to get information like username, credit cards details and passwords by pretending to be a reliable company (Abdullah and A.K, 2004). In 1995, first phishing incident was observed (Bose et.al,2007). Rapid increase in Phishing has caused significant losses to business sector around the globe (Lininger and Vines, 2005). In year 2004 there were about US$ 1.2 billion of financial loss that caused by 1.8 million phishing attacks (Geer,2005) and more than 5 million U.S. customers missing money to phishing attacks in the 12 months ending in September 2008 (Gartner, 2009). Phishing attacks around the world cost billions of dollars in loss every year (Mc Combie et.al, 2009). Phishing has a huge negative impact on organizations' client relationships revenues, marketing pains and general corporate appearance (Dhanalakshmi et.al, 2011). Statistics report that 35.9% of financial sector is the target of Phishing frauds (APWG, 2010).

Research has examined the effects of a globally deviate view on criminal laws as it relates to the apprehension and trial of cyber criminals (Brenner and Koop, 2004). The burden of proof of online fraud is a discouraging task for an normal internet user. In 2005, a Miami capitalist filed a lawsuit against the bank of America. Money had been shifted out of the plaintiff's bank account; the fraudster was able to get the businessman's account details through a key-logging virus which had infected the plaintiff's computer. The Bank of America said that they were not liable for the theft and removal, as the removal had been completed with appropriate handling and security measures and their own systems were not subject of hacking. The plaintiff said the bank was careless and should have "let him know of the virus risk prior to the transfer" (The Banker, 2005). If the normal internet user cannot take remedy from the bank, reporting future incidences will become discouraging. Numerous government agencies around the world have taken necessary precautions to detect and persecute committers of cybercrime. Due to the vast amount of new technology being produces regularly government agencies have to stay alert and informed in order to control the cybercrime. Cybercrime can be victimless, but it can also hurt unlucky individuals.

Pakistan government is trying its best to digitize public sector. Several initiations have been undertaken to help the digital boom in the private sector. Recently government has launched 3G and 4G technology, which will bring a revolutionary change in the telecommunication sector. Moreover, huge amounts are allocated to support the e-Government, e-Banking and e-Learning in the country. However, no proper legislation is made to prevent the electronic/cyber-crimes to protect the users from e-frauds etc., which is a major barrier towards trust and confidence of the users. Though, the Pakistan Electronic Crimes Ordinance (2002) modified (2008) were circulated, however these failed after six weeks under the constitution of 1973. Moreover, Pakistan Electronic Crimes Act (2007) and now Pakistan Electronic Crimes Act (2014) have been introduced as draft law but still waiting to become law, thus in the absence of cyber-law, cyber criminals are enjoying to play with online community, who are easily falling their victims, losing not only their privacy, data and money but also in some cases, damage to their social and family life (Magalla, 2013).

In addition to the previous laws, government has offered a new draft law titled as Prevention of Electronic Crimes Act 2014 before cabinet for approval, which proposes some strict punishments for cyber-crimes; however, it is lacking because it leaves all offences as bail able (Jamil, 2006). This proposed draft of law shall cover cyber terrorism, unauthorized intervention, illegal access to information system and program or data, illegal intervention with program or data, electronic falsification, identity crime and protection of women etc. Thus, in the absence of cyber-crime laws through which punitive action could be initiated against those criminals who will be committing crimes on the cyber world in Pakistan, individual and organizations both public and private are increasingly becoming victims of abuse on social media sites and internet frauds, etc. (Chaudhy,2011; Bell, 2002; Grabosky et al., 2001).

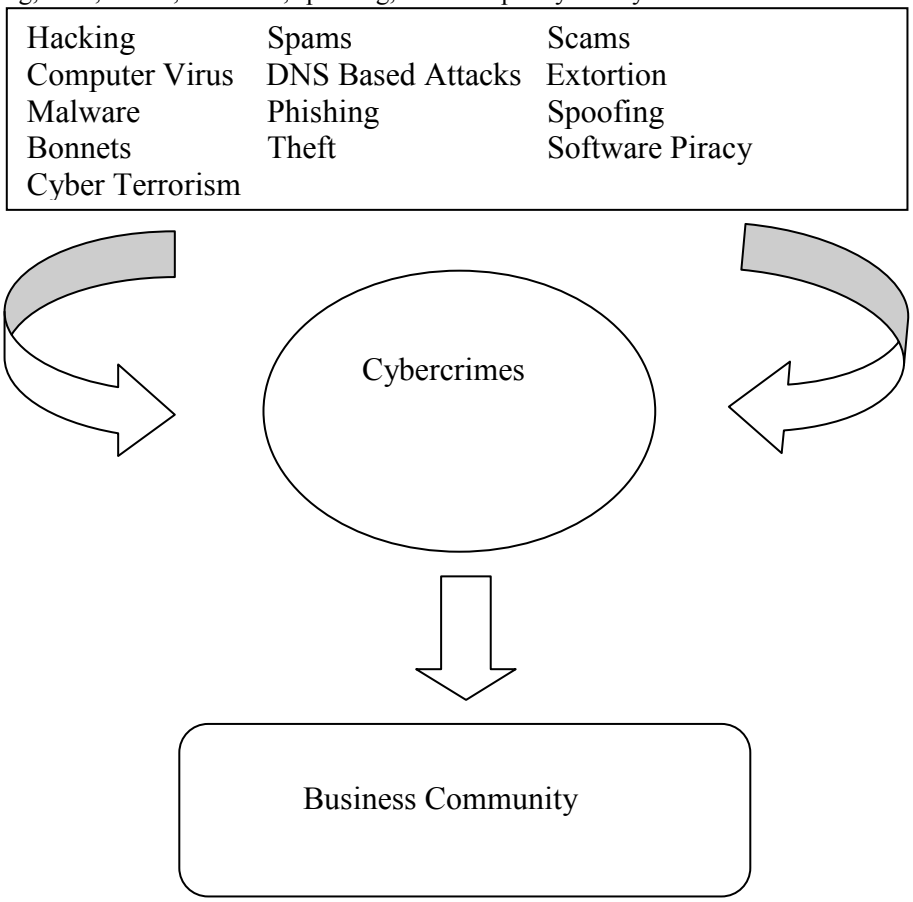
2. Methodology

Methodology used is empirical and data is collected from the all districts of the Southern Punjab which consists of Dera Ghazi Khan, Bhawalpur, Multan, Rahim Yar Khan, Bhawalnagar, Ranjanpur and Layyah. Data is

collected through questionnaires and interviews. The selected population for this study is business community of Southern Punjab. The fifty likert scale questionnaires were serve to collect the data from targeted population. The response rate was 100%.The collected data is analyzed through quantitative techniques by using SPSS software.

3. Conceptual framework

The conceptual frame work contains those factors that may effect the business community and are the great hindrance between business community and e-business in the Southern Punjab. Main factors of the model that influence the E-business in Southern Punjab are hacking, computer virus, malware, bonnets, spams, DNS Based attacks, phishing, theft, scams, extortion, spoofing, software piracy and cyber terrorism.



Conceptual framework of the research

The business community is dependent variable while all others are independent.
Additive model is used here. Equation of the model is given as,

$$Yi = \beta_0 + \beta xi + \varepsilon i$$

Here is, Yi represents the dependent variable, β_0 denotes the constant, β is regression coefficient of independent variables, xi represents the independent variables also called as explanatory variables and εi denotes the random error. So equation representing our conceptual frame work is given as,

$$BC = \beta_0 + \beta\ (CCs) + + \varepsilon i$$

Here is, BC represents the dependent variable business community while β (CCs) is independent variable represents the cybercrimes.

4. Hypothesis

Business community is dependent variable while the cybercrimes are independent variables. Following hypothesis is constructed on the basis of conceptual framework.

H_1: Cybercrimes have a positive and significant relationship with electronic business in business community of Southern Punjab, Pakistan.

5. Data analysis

Model summary

Model	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.807	0.863	6.2453

a. Predictors: (Constant), CCs

The R2 in the model is 0.807 which means that the independent variables can explain 80.7% of change in the dependent variable. The adjusted R2 demonstrates that 86.3% of the variances between dependent and independent variables in this model.

Table-1 Model Summary of the Variables

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	4004.593	1	4004.593	73.567	0.000[b]
	Residual	581.064	48	41.961		
	Total	5586.567	49			

a. Dependent Variable : BC

b. Predictors: (Constant), CCs

Table-2 ANOVA Analysis of the Variables

The researcher used one variable that is acting as independent variable and model shows the significant impact of this variable on dependent variable business community of Southern Punjab, Pakistan.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.632	2.521		2.601	.000
	CCs	3.561	0.509	.959	8.386	.002

a. Dependent Variable: BC

Table-3 Regression Analysis of the Variables

Beta explains the contribution of independent variable cybercrimes CCs with beta coefficient of 3.561 and sig. value of .002 makes the strong contribution in explaining the e-business of business community BC. The independent variable shows impact on dependent variable business community significantly. The statistical tests applied in this case, also suggest there is a strong relationship between independent variables and dependent variable.

Correlations analysis

Correlation		BC
CCs	Pearson Correlation	.959**

**Correlation is significant at the 0.01 level (2-tailed).

Table-4 Correlation Analysis of the Variables

Result declaring significant correlation =.959 because value is falling between -1 to +1.

The regression analysis shows that there is a significant impact of independent variable on dependent variable business community. Also the correlation analysis shows that the correlations between variable is as follows, the variable has correlation significant at 0.01 levels with each other. The results of correlation and regression analysis support our hypothesis i.e., the factors cybercrimes have a significant and positive relation with dependent variable business community regarding e-business in Southern Punjab, Pakistan.

6. Conclusions and recommendations

E-business is facing many challenging regarding cybercrimes in Pakistan due to several reasons fluctuating from the deprived technology, ineffectiveness and lack of legislation to financial limitations, lack of cooperation with international law and enforcing agencies. Cybercrime is known to all over the world as a crime committed through the internet. It is, now a days, becoming a serious matter of concern all over the world. From the above data the researcher concluded that the hindrance in the e-business in Southern Punjab is cybercrimes. The most of the business community are not well educated, but they have done online money transactions like easy paisa and use of ATM. They do not use their credit or debit cards for online sale and purchase due to the danger impact of hacking of passwords. So our hypothesis is true and cybercrimes have a positive and significant impact on the business community of Southern Punjab, Pakistan regarding online sale and purchase or e-business.

Technology based crimes have been developed with the passage of every day. And they must be handled with the supreme importance. These crimes are not narrow to computers, but other electronic equipments are made its means such as financial transaction machines, telecommunication equipment's and so on. The legislative reforms will be more effective if they would be completed according to nature of cybercrime, so that maximum punishments are possible and no one would be able to escape from the hands of law and courts

just due to unavailability of a specific law. Developing countries are trying to fight against cybercrime with their minimum resources. Developed countries should feel their responsibility and facilitate developing countries as much as possible because if cybercrimes are not controlled now then it will affect the whole world with a single click. Countries facing the cybercrimes should focus on latest technology for investigation of these crimes to collect the evidence of any crime as much as possible. The Government should take concrete steps with their minimum resources towards the reduction of the cybercrimes.

References

1. Abdullah, A.-K. (2004). "Protecting your good name: identity theft and its prevention". In Proceedings of the 1st annual conference on Information security curriculum development (pp. 102–106). New York, NY, USA: ACM. doi:10.1145/1059524.1059547
2. ACPR. (2004). Parliamentary joint committee on the Australian crime Commission. Retrieved from http://www.acpr.gov.au./pdf/ACPR145_2.pdf
3. ACPR. (2006). Parliamentary joint committee on the Australian crime Commission. Retrieved from http://www.acpr.gov.au./pdf/ACPR145_2.pdf
4. APWG ; Retrieved from http://www.antiphishing.org/ (Accessed on April 2015)
5. Barr, R. & Pease, K. (1990). Crime placement, displacement, and deflection", in: M. Tonry & N. Morris (eds), *Crime and Justice: A Review of Research*, 12(3): 12-23, University of Chicago Press, Chicago.
6. Bell, R.E. (2002). The prosecution of computer crime, *Journal of Financial Crime*, 9(2): 308-25.
7. Blindell, J. (2006). Review of the legal status and rights of victims of identity theft in Australasia. Retrieved from http://www.acpr.gov.au./pdf/ACPR145_2.pdf
8. Brenner, S. & Kopops, B. (2004). Approaches to Cybercrime Jurisdiction. *Journal of*
9. Brenner, S. W., & Goodman, M. D. (2002). Cybercrime: The Need to Harmonize National Penal and Procedural Laws. Retrieved from http://www.isrcl.org/paper/brenner.pdf
10. Chaudhy, Y. (2011). A country without cyber-law: Pakistan, [Online] available at:
11. Convention on Cyber-Crime. (2001). The Convention on Cyber- Crime, a unique instrument for international co-operation. Budapest: Council of Europe. Retrieved from http://conventions. coe.int/ treaty/ EN/projets/ projets.htm.
12. Gartner. (2009, April). "Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008". Retrieved from http://www.gartner.com/newsroom/id/936913
13. Geer, D. (2005). "Security technologies go phishing". Computer, 38(6), 18 – 21. doi:10.1109/MC.2005.201 James, L. (2006). Phishing Exposed (1st ed.). Syngress.
14. Gjata, O. (2007). Cybercrime. Retrieved from http://mason.gmu.edu/~ogjata/index.html
15. Grabosky, P.N., Smith, R.G., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace*, Cambridge University Press, Cambridge.
16. Graycar, A. (2000). Nine types of cyber crime. Retrieved from http://aic.gov.au/conference/ other/graycer_adam/2000-02-cybercrime.html.
17. *High Technology Law*, *4*(1), 3-44.
18. http://propakistani.pk/2011/01/10/a-country-without-cyber-law-pakistan/10,june 2011/, (March 24, 2015).
19. Jamil, Z. (2006). *Cyber Law*, Presented at the 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August, 2006, Jamil and Jamil Law Associates, Islamabad, Pakistan, [Online] available at: http://jamilandjamil.com/wpcontent/
20. Jason Milletary (2005), Technical Trends in Phishing Attacks, CERT Coordination Center1, pp. 1-17.
21. Kowalski, M. (2002). Cyber Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics. Catalogue No. 85-558-XIE, ISBN 0-660-33200-8. Retrieved from http://statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf
22. Lininger, R., & Vines, R. D. (2005). "Phishing: Cutting the Identity Theft Line" (1st ed.). Wiley.
23. Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, *9*(3), 155-165.
24. Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, *9*(3), 155-165.
25. Magele, T. (2005). *E-security in South Africa*, White Paper prepared for the ForgeAhead e-Security event. Retrieved March 20, 2015, from www.forgeahead.co.za/.
26. McCombie, S., Pieprzyk, J., & Watters, P. (2009). "Cybercrime attribution : an Eastern European case study" |Macquarie University ResearchOnline, Cybercrime attribution : an Eastern European case study. Retrieved from http://www.researchonline.mq.edu.au/vital/access/manager/ Repository/mq:12626
27. Oumarou, M. (2007). Brainstorming advanced fee fraud: 'Faymania' – the Camerounian experience. In N.

Ribadu, I. Lamorde, & D. Tukura (Eds.), *Current trends in advance fee fraud in West Africa,* EFCC, Nigeria, 33–34.
28. Pati, P. (2003). Cybercrime, New Delhi. Retrieved February 23, 2015, http://www.naavi.org/
29. pati/pati_cybercrimes_dec03.htm.
30. R. Dhanalakshmi, C. Prabhu, C. Chellapan (2011). Detection Of Phishing Websites And Secure Transactions , *International Journal of Communication Network and Security* (IJCNS-), Volume. 1 Issue. 2.
31. Richardson, R. (2008). *2008 CSI Computer Crime and Security Survey*, Computer Security Institute. Retrieved April 12, 2015, from ttp://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf
32. Salifu, A. (2008). Impact of Internet crime on development. *Journal of Financial Crime, 15*(4), 432–444.
33. The Banker (2005, March). Lawsuit raises online fraud issue for banks. *The Banker*, p.12.
34. uploads/2010/11/article_for_scp_50_anniv_v5.0.pdf, (March 16, 2015).
35. Williamson, Gregory D (2006). Enhanced Authentication In Online Banking, Journal of Economic Crime Management, Vol. 4, Issue 2.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar