Global Journal of Management, Social Sciences and Humanities 821
Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

THE IMPACT OF CYBERCRIMES ON THE EFFICIENCY OF BANKING SECTOR OF PAKISTAN

Prof. Dr. Shaukat Malik[1], Shazia Noreen[2], Prof.Dr.Abdul Ghafoor Awan[3]

ABSTRACT: This research examines the impact of cybercrimes on the efficiency of Banking Sector of Pakistan. For this purpose, ten banks of Pakistan are considered as sample for data collection. Questionnaire is employed to collect and analyze the primary data for drawing the results. Correlation analysis and Likert Scale were used to measure the impact of cybercrime on the performance of banks. The empirical results reveal that cybercrimes have negative and significant impact on the efficiency of banks of Pakistan. Our results further reveal that Government policies may also lessen the impact of cybercrimes but not to higher limit. We suggest that special focus may be given to the causes of the cybercrimes.

Key words: Cybercrimes, Efficiency, negative impact, performance of banks, Economic growth, Rate of cybercrime.

Type of study: **Original Research paper.**

Paper received: 15.07.2018
Paper accepted: 26.08.2018
Online published: 01.10.2018

1. Director, Institute of Banking and Finance ,BZU Multan-Pakistan. shoukatmalik@bzu.edu.pk. Cell # 0923006302202.
2.MS Scholar, Department of Business Administration, Institute of Southern Punjab, Multan Pakistan.
3.Dean, Faculty of Management and Social Sciences, Institute of Southern Punjab. ghafoor70@yahoo.com. Cell # +923136015051.

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

1.INTRODUCTION

The word 'Cyber' stands for computer generated and 'crime' means any unlawful or illegal activity done by an individual for the violation of public rights which may be punished for it. In this way cybercrime is a criminal activity through computer or the Internet. Cybercrime is also known as computer crime; new technology always makes new criminal opportunities and some new types of crimes always. One difference is that cybercrime is the use of digital computers in contrast to traditional criminal activity. Most Common cybercrimes include data theft, extortion, fraud and identity theft.

Cybercrime or computer crime has become an important area of interest these days. Recent media coverage has dealt with the widespread stories of substantial scale information ruptures, hacking and numerous online monetary wrongdoings. Currently, the number of cybercrime occurrence is in increasing day by day, as this number is almost always depicted in either absolute 1000 attacks per year or this percentage may change year-over-year (50% more attacks in 2014 than in 2013). Recent discussions of 'cybercrime' focus upon the apparent novelty or otherwise of the phenomenon. The major actions regarding the usage of computers and computer networks to commit criminal activities started in 1970's and are continues to the present day. The first Cybercrime started in 1820 with hackers trying to break into computer networks.

1.2 STATEMENT OF PROBLEM

In today's world, cybercrimes are a big threat to the whole business world. In fact, not a single company is completely immune to it (Olorunsegun, 2010). Public expects complete responsiblity, fairness, transparency and effective communication from banks. All the banks expect to make sure that they fulfill their responsibilities

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

with sincerity which can be innocent of dishonorable activities. Instead of great care, there are many known cases of online frauds in the banking sectors of Pakistan. A main question arises that what is the impact of cybercrimes on the efficiency of banks of Pakistan? This is the problem that necessitates this research study.

1.2 OBJECTIVE OF THE STUDY

The objectives of study are stated as under:-

1. To find out the impact of cybercrimes on the efficiency of ten banking sectors of Pakistan.
2. To identify the main types of cybercrimes severely threatening the banking sectors of Pakistan.
3. To ascertain the main factors encouraging people involvement in the cybercrime activities.
4. To identify measures that will be helpful in cybercrimes prevention.

1.3 Research questions

This research study will explore answer to following questions:

1. What is the impact of cybercrime activities on the efficiency of ten banking sectors of Pakistan?
2. What are the main types of cybercrimes severely threatening the banking sectors of Pakistan?
3. What are the main factors encouraging the people involvement in cybercrime activities?
4. What measures banks should or have taken to prevent from cybercrimes?

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

1.4 Scope of study

Cybercrimes are the major challenge to the whole working organizations. All the businesses worldwide have been affected through cybercrimes. According to a study currently done, the cybercrime occurrence rate in Pakistan is lower than US and other developed countries. This study is useful for identifying the impact of cybercrimes on the efficiency of banking sectors in Pakistan and in other countries.

2. LITERATURE REVIEW

Computer is the main tool used for criminal activity. Where cybercrime highlights the severity of the computer networked in our lives; it clearly identifies such obvious strong facts as personal identities. As a proof of technology developed by the natural world of crimes, all these crimes are new, unless the computer is in existence, which describe non-social societies and is generally meant to fight against the world, crime. In 1996, the European Council, the United States, Japan and Canada's official representatives signed an initial agreement for the crime of computer internationally.

According to the DOJ which is U.S department of Justice, "Cybercrime" refers to any illicit action that a computer is employed as its primary suggests that of transmission, commission, and storage. The SA policy definition- National Cyber Security Policy Framework for South Africa on 07-03-2012 states: "Cybercrime" means unlawful actions; its commission includes the use of communication and information technologies.SA Law proposed new definition-Electric communications and Transactions Amendment Bill (26th of October 2012) states:

"Cybercrime" "is any criminal or other offence that is facilitated by or involves the use of an electronic communication or information system. It includes any device or

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

the internet, any one or more of them". Lord Atkin says: "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime".
According to Josh Wepman "Cybercrime is one of the fastest growing crimes at international level.

K. Jaishankar and Debarti Halder defined cybercrimes from the standpoint of gender. They defined, "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones are called 'Cybercrimes against women". Attack on information about most cybercrime individuals, corporations or gurus are attacked. Although these attacks cannot be placed on the physical body, it is on a personal or corporate virtual body, which defines the characteristics of information that defines the people and organizations that die on the internet. In other words, in this digital era, our virtual identity is essential elements of daily life: we recognize advertisements and numbers and identities in many computer databases of governments and corporations. Where cybercrime highlights the severity of the computer networked in our lives, it clearly identifies such obvious strong facts as personal identities. Cybercrimes could intimidate an individual or a nation's security system and money health of any country. Internationally, each government and non-state players interact in cybercrimes together with money larceny, spying and alternative cross-border crimes. associate act crossing the international borders and that involves the interests of a minimum of one nation state is usually referred as cyber warfare.

According to data obtained about cybercrimes in Pakistan, software piracy costs over $ 315b per year (Pakistani observer). According to The News International

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

2014, anti-malware war cost $ 500bn in 2014. According to a survey report; nearly ten to fifteen cases area unit registered each day what might begin from hacking a customer's account to dangerous results comparable to illegal and unauthorized fund transfer and withdrawal from user's account while not his or her permission. Pakistan, that is o the 67th variety on the worldwide Cyber Security Index 2017, faced recently a modern law-breaking attack. Once 559 Habib Bank Ltd Accounts were hacked through ATM cards in China and Rs ten.2 million were purloined.Consultants at a conference organized by West Pakistan Academy of Engineering (PAE), titled "Cyber Security- wherever can we stand"?, same on Sat. it should result to negligence or incompetence of the govt., banks and state establishments that they didn't traumatize the threats of on-line monetary frauds even when some Chinese nationals were caught whereas putting in skimming devices at ATMs of Bank Al-Habib in city in Jun, 2016. Consistent with PAE President Dr. Jameel Ahmad Khan at Saturday's event, the web is growing quicker however the govt. or industry's ability isn't compatible to secure it. Consistent with earlier statement, the country's banking sector was the foremost susceptible to cybercrimes; Khan extra that the monetary establishments had enough resources to manage the system to stay up with the worldwide network.

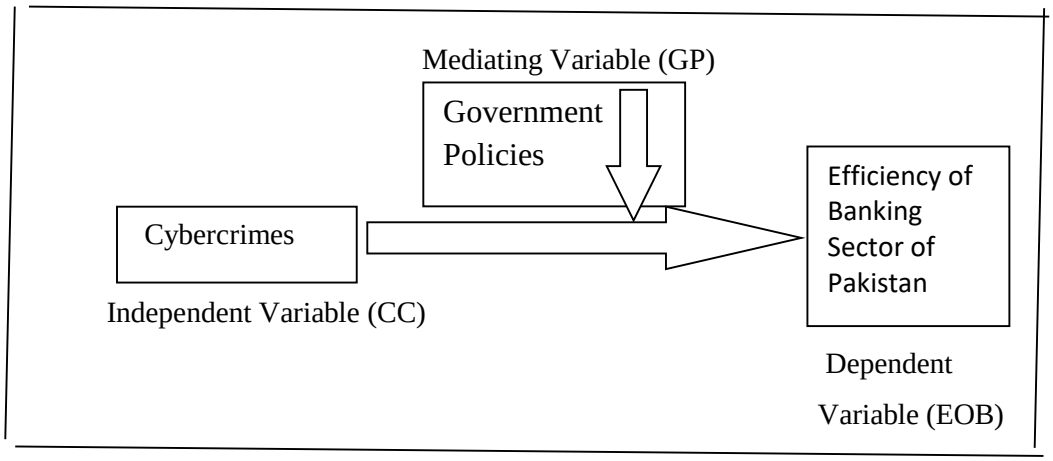
3.CONCEPTUAL FRAMEWORK

On the left side of this diagram, is the independent variable is mentioned which are "cybercrimes". These can be classified into different types such as cyber stalking, child pornography, email spoofing and hacking etc. Further types are already explained in detail so that we may be able to know which type is more dangerous and which has much frequency for happening. In this way, we may also identify the impact of these variables (cybercrimes) on the banking sector of Pakistan.

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

On the right side is the efficiency of the banking sector f Pakistan which is dependent variable. As we already discussed efficiency of banking sectors of Pakistan is affected by the cybercrimes which are independent variables. But when Govt makes policies to overcome cybercrimes, there will be change in the efficiency of banking sectors of Pakistan, Government policies in this framework work as controlling variable.

Figure.1 Sketch of Model



3.1 HYPOTHESIS DEVELOPMENT

The above mentioned conceptual framework provides the foundation for hypothesis development. We have formulated two hypotheses on the bases of data collection for this research and findings of previous research. First is the null hypothesis and second is the research hypothesis which are mentioned below.

Ho: Cyber Crimes have no impact on the efficiency of the Banking Sectors of Pakistan.

H1: Cyber Crimes have impact on the efficiency of the Banking Sectors of Pakistan.

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

4. RESEARCH METHODOLOGY

The main purpose of this research is to analyze the impact of cybercrimes on the efficiency of banking sectors of Pakistan. So, for this purpose we have taken banking sector of Pakistan. All the banks are taken as population while 10 banks are selected as sample named HBL, UBL, Faysal Bank Ltd, Askari Banlk Ltd, BOP, Bank Al-Habib, Muslim Commercial Bank Ltd, The First Micro Finance Bank Ltd, ABL and Meezan Bank Ltd. The data for sampling is collected for the year 2018.

4.1 VARIABLES

Three variables are used in this research. Cybercrimes are the independent variables, efficiency of baking sectors is dependent variable and Govt policies are the controlling variable.

Table 1: Summary of variables used in Research

No.	Variables	Code	Measures
1	Cybercrimes	CC	Effectiveness of Cybercrime
2	Govt. Policies	GP	Effectiveness of Govt Policies
3	Efficiency of Banks	EOB	Change in the efficiency of Banking sectors of Pakistan

4.2 Research Techniques

Quantitative research method is used in this research. The whole data is collected and analyzed through primary research and data collection tool used is questionnaire which was filled by each sample bank. Likert scale is used as measurement tool. Correlation analysis was also applied to check for the relationship between dependent and independent variables.

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

5. DATA ANALYSIS

We surveyed ten banks for data collection for our research trough questionnaire. Through this research we got the data related to the research topic to analyze our hypothesis which is that are the cybercrimes have impact on the efficiency of banking sectors or nor? We analyzed data and got results which are mentioned in the form of Tables and charts. The results are shown in Table 2 on next page.

Global Journal of Management, Social Sciences and Humanities 830
Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

Q.No and detail	Name of Banks (Data for the year 2018)									
	HBL	UBL	ABL	BOP	MCB	Faysal Bank Ltd	Askari Bank Ltd	Meezan Bank Ltd	Bank Al-Habib Ltd	First Micro-finance Bank Ltd
1. How much people know about cybercrimes ?	4	2	2	2	2	2	2	4	3	2
2. To what extent we can measure cybercrimes ?	2	4	3	1	3	4	2	3	4	3
3. To what extent cybercrimes really occur in Pakistan?	4	5	4	2	4	4	5	3	3	4
4. What is the rate of cybercrimes occurrence in Pakistan?	4	4	4	3	4	1	4	5	4	5
5. To what extent this rate growing day by day?	5	5	5	4	4	4	4	4	3	4
6. To what extent Govt policies are effective in reducing cybercrimes ?	2	2	3	1	1	4	3	4	3	5
7. Does cybercrimes really impacts the efficiency of banking sectors of Pakistan?	5	5	4	4	4	4	5	5	4	5
8. To what extent the cyber crime is really a burning issue to	5	5	4	3	4	4	4	5	4	5

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

damage the progress of banking sectors of Pakistan?										
9. How much cybercrimes impact the efficiency of banking sectors of Pakistan?	4	4	5	3	3	2	3	5	3	5
10. To what extent does the age really matters in committing cybercrimes ?	2	3	5	3	2	4	5	3	4	3
11. To what extent should we take some measures to avoid from cyber crimes?	3	5	4	3	5	4	5	5	4	5
12. To what extent should we take some measures to avoid from cyber crimes?	4	5	4	1	5	4	5	5	4	5
13. To what extent should we take some	5	5	4	5	4	3	4	4	3	4

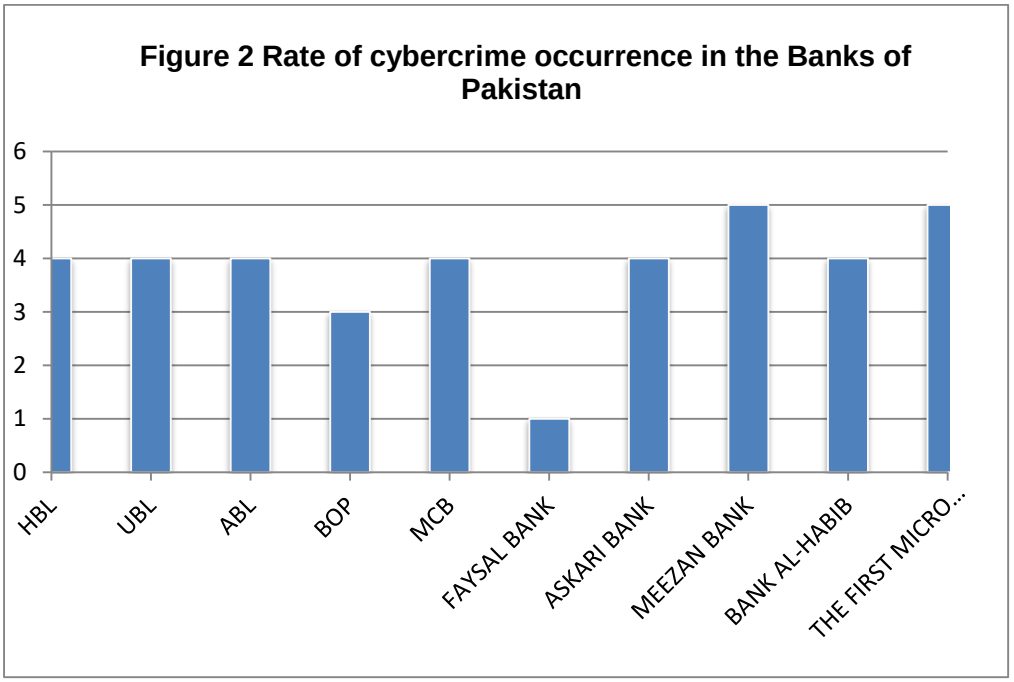
Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

measures to avoid from cybercrimes ?										
14. Which factor mostly forces the people to commit cybercrimes ?	Getting prohibited information	Greediness	Revenge	Greediness	Greediness	Greediness	Greediness, Destructive mind set, getting prohibited information	Greediness	Revenge	Revenge
15. Which type of cybercrime is frequently occurring in Pakistan recently?	Identity theft	Carding	Identity Theft	Identity theft	Carding	Hacking	Hacking,identity theft, carding	Identity Theft	Carding	Denial of service attack
17. Is any cybercrime committed in your organization ?	Yes	No	Yes	No	Yes	No	No	Yes	Yes	No
18. What was the extent of occurrence of that cybercrime?	3	-	4	-	3	-	-	2	4	-

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

According to this research 50% people know about Cybercrimes. Cybercrimes can be measured till 58 % rate. There are 76% chances that Cybercrimes are really occurring in Pakistan.

The overall rate of occurring cybercrimes in Pakistan was 76% till April 2018. This rate separately for each bank can also be presented in the form of chart.

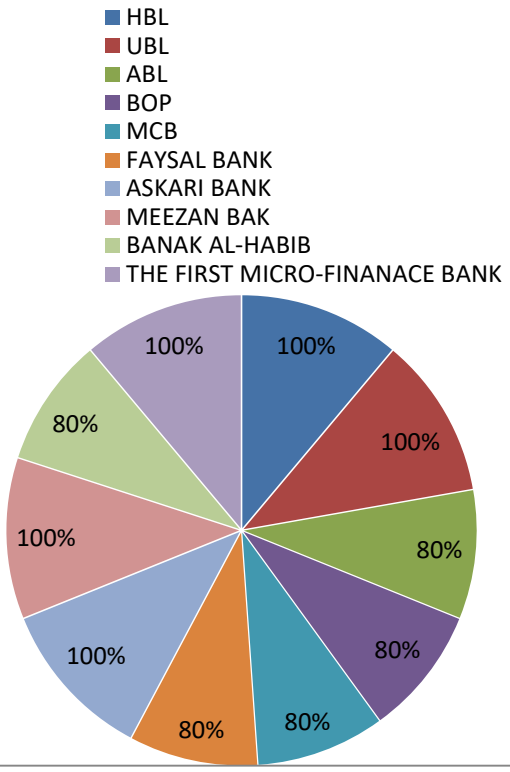


Banks names are mentioned on X-axis and Likert scale readings are showed on Y-axis. According to research this rate is increasing day by day by 84 %. By this research we have found out that Government policies are effective in reducing the cybercrimes but not too much extent (56%).

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

This research proved that the overall extent of cybercrimes really impacting the efficiency of banking sectors of Pakistan is 90%. This can be separately showed in the form of Pie chart.

Figure 3 The effect of cybercrimes on efficiency of banks.



Impact of cybercrimes on the efficiency of HBL, UBL, Askari Bank, Meezan Bank and The First Micro-Finance Bank is 100%.On ABL, BOP, MCB, Faysal Bank,

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

and Bank Al-Habib, it is 80%. And in this way this research proves our hypothesis H0 wrong that cybercrimes have no impact on the efficiency of banking sectors of Pakistan. And the hypothesis no.1 comes true that cybercrimes really have an impact on the banking sectors of Pakistan. 82% banks agree that Cybercrime is really a burning issue to damage the progress of banks of Pakistan. We also learnt from this research that age also matters in committing cybercrimes and this percentage is 68%.As the cybercrimes really lower the performance of banking sectors we should take some measures to avoid too much lose occurred due to cybercrimes.86% people have opinion That we really should take some strong measures to avoid from cybrcrimes.20% people commit cybercrimes to get prohibited information.30% people commit cybercrimes due to revenge. Only 10% people do cybercrimes due to destructive mindset. The percentage of people committing cybercrimes due to greediness is 60%. Which is biggest rate than all other factors (revenge, getting prohibited information, destructive mindset) forcing cybercrimes.

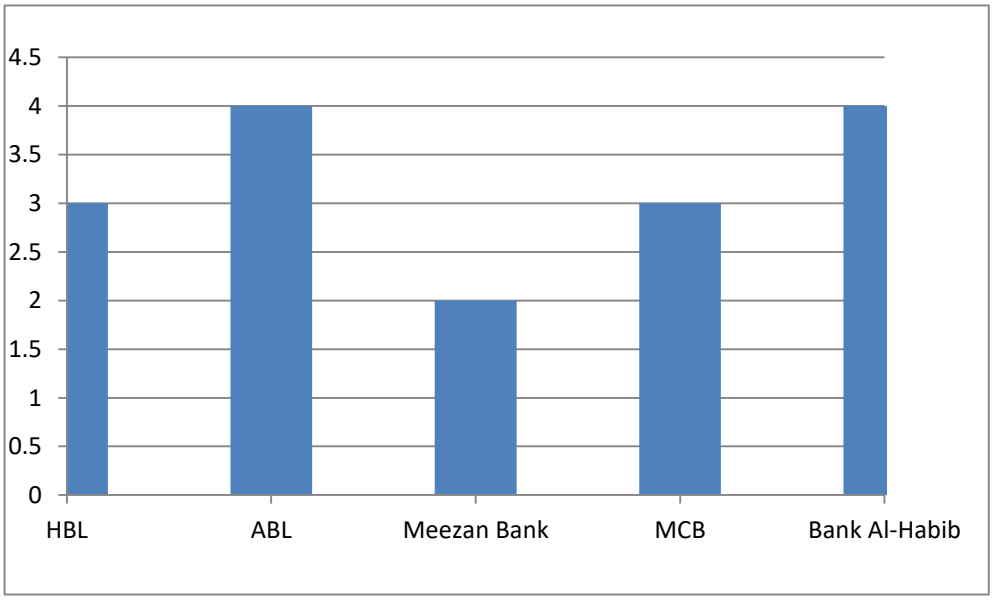
When we talk about the type of cybercrimes occurring in Pakistan in the given ten banks (2018), we got information that the most frequently occurring type of cybercrime in these ten banks has been identity theft which is 40%.Carding is 30%.Hacking is 10% and Denial of services attack is also occurring at the rate of 10%.

Now we mention the banks in which cybercrimes were committed from 2013 to 2017.From the list of ten banks named HBL, UBL, Askari bank, MCB, ABL, The First Micro Finance Bank, Meezan Bank, Faysal Bank, BOP and Bank-Al Habib which we have taken as a sample in our research, the banks in which cybercrimes occurred (2018) were HBL, MCB, ABL, Meezan Bank and Bank-Al Habib. In HBL

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

and MCB severity of occurrence was 60%.In ABL and Bank-Al Habib it was 80% and in Meezan bank it was not severe attack of cybercrime. Its extent was 50%. Banks in which cybercrimes are occurring with high ratio, can also mentioned below in bar chart form. Five banks are mentioned in which cybercrimes are recently committed and their extent of occurrence.Banks names are mentioned on X-axis. While Likert scale is showed on Y-axis.

Figure 3 Frequency of cybercrimes in banks



These are the five banks; HBL, ABL, Meezan Bank, MCB and Bank Al-Habib in which cybercrimes have been occurred in 2018.And the rate with which they are committed is also mentioned on y-axis.

5.1.Measures opted by banks to control Cybercrimes (Justification of Q.19 &20)

We also learnt about different measures, systems or software which are adopted by these banks to minimize cybercrimes has a separate IT Deptt to handle

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

cybercrimes. It isolates the infected workstations from network with the help of IT experts, it installed the Security Patches, upgrade the OS version with latest Security Patches. It executes the deep scanning to identify and remove the infected items. UBL has strong IT team which is helpful to avoid risks. It has strong firewall system. In UBL anti-fraud unit is also established to overcome cybercrimes. According to this research MCB has no specialized IT Team. It updates its KYC and AML regularly. It organizes training sessions and fresher courses to provide awareness about cybercrimes and how to avoid from cybercrimes. The First Micro Finance Bank has proper firewall system and proper monitoring of items where possibility of cybercrimes occurrence. ABL is has Anti-skimming software and firewall system. It also has FMRU Deptt and fraud management and restriction unit to minimize cybercrimes. BOP has IT experts and also firewall system to overcome cybercrimes. Faysal Bank has specialized IT team for this purpose. It takes measures through education to its staff and customers, awareness through mails and SMS. It also controls cybercrimes through firewalls and information secrecy system. Bank-Al Habib has IT team. It overcomes cybercrimes through proper monitoring (ATM), awareness to its staff and customers and by using firewalls. Askari bank protects its bank from cybercrimes through proper check and balance and by using firewall system. Meezan Bank has IT specialists who monitor different tasks and have complete control over all the functions of systems so that if something unfavorable occurs they may control it.

6.CONCLUSIONS

The main Purpose of this research was to examine the impact of cybercrimes on the efficiency of the banking sectors of Pakistan. For this purpose, we studied different articles and investigations made by different researchers to explore the

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

impact of cybercrimes on the efficiency of banks in the world as well as in Pakistan. Though the banks of Pakistan are the well-organized industry but as the world are affected by the cybercrimes so as to the banking sectors of Pakistan. For the purpose of our studies, we selected ten banks and collected data through questionnaire. Likert scale was used to measure the extent. We made two hypotheses H0 which was that cybercrimes do not have any impact on the banking sectors of Pakistan. And the other was H1 that cybercrimes have a impact on the efficiency of banking sectors of Pakistan. This research through questionnaire not only testified our hypothesis but also provided us with bunch of information about cybercrimes.

The research results revealed that cybercrimes really have an impact on the efficiency of banking sector of Pakistan. And those negatively affect the banks of Pakistan. In this way, they lower the banking profits, trust of customer and ultimately economic growth of Pakistan. Results also revealed that governmentt policies are efficient in reducing cybercrimes but still need more enforcement. Findings of this research also revealed about the extent, occurring rate, and severity of damage due to cybercrimes. Results also revealed about the occurrence of cybercrimes in different banks and most frequent types of cybercrimes and how much age matters in committing cybercrimes. We knew through this research that recently, in five banks cybercrimes were occurred and severity was 60-80%. We also learnt about the factors which mostly become the cause of cybercrime occurrence.

7. RECOMMENDATIONS

This research gave us knowledge about how these ten banks are taking measures to reduce or control cybercrimes. Mostly these banks have hired IT experts to protect their system. Commonly firewall is used to protect from cybercrimes. More awareness is to be given to people about cybercrimes and damage incurred due to it.

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

Different new software be used in different banks to overcome cybercrimes. Every bank though struggling in different ways to control and avoid from cybercrimes. But still there is dire need to improve it more.

REFERENCES

Adeoti, J.O (2011), Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out", *Journal of Social Sciences*, 21(1), pp 53-58.

Aderibigbe, P.(1999),The Internal Audit Function and Fraud: A Nigerian Case Study", *ICAN News*, January/March, pp 15-19.

Adeyemo, K.A. (2012), Frauds in Nigerian Banks: Nature, Deep-Seated Causes, Aftermaths and Probable Remedies", *Mediterranean Journal of Social Sciences*, 3(2) pp 279-289.

Aruna Devi (2017), "chapter 11 Cyber Crime and Cyber Security", IGI Global.

Bell, R.E. (2002). The prosecution of computer crime, *Journal of Financial Crime* , 9(2): 308.

Awan, Abdul Ghafoor; Sahar Saeed (2015). "Conflict Management and Organizational Performance: A case study of Askari Bank Ltd", *Research Journal of Finance and Accounting*, Vol 6 (11): 88-102.

Awan, Abdul Ghafoor;Syed Zuriat-ul Zahra (2014) "Impact of Innovation on consumers' behavior: A case study of Pak Electron Limited" European Journal of Business and Innovation Research, Vol 2 (6):93-108

Barr, R. & Pease, K (1990). Crime placement, displacement, and deflection", in: M. Tonry & N. Morrism(eds), Crime and Justice: *A Review of Research*, 12(3): 12-23, *University of Chicago Press*, Chicago.

Chapman, A.,& Smith, R.G. (2001). Controlling financial services frauds, Trends and

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

Issues in Crime and Criminal Justice, 2: 189, *Australian Institute of Criminology*, Canberra.

Clarke, R.V & Weisberg, D. (1994). Diffusion of crime control benefits : Observations on the reverse of displacement, in: R.V. Clarke (ed.), Crime Prevention Studies, 2: Willow Tree Press, Monsey, New York.

Collin, B. (1996). "The future of cyber terrorism", Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, Denning, D. E. (2001) Cyber warriors: Activists and terrorists turn to cyberspace. *Harvard International Review*, XXIII (2)

Ghauri, I. (2014). Electronic Crimes Act: Cybercrime to be made non-cognizable offence, The Express Tribune with the International New York Times.

Grabosky, P.N & Smith, R.G. (1998). Crime in the digital Age: Controlling telecommunications and cyberspace illegalities, Federation Press, *Sydney/Transaction publishers*, New Brunswick.

Grabosky, P.N.,Smith, R.G., & Dempsey, G. (2001). Electronic theft: Unlawful acquisition in cyberspace, *Cambridge University Press*, Cambridge.

Grandjean, C. (1990). Bank robberies and physical security in Switzerland: A case study of escalation and displacement phenomena, *Security Journal*, 1:155-9.

Hakim, S & Rengert, G.F (1981). Introduction, in: S. Hakim & G.F. Rengert (eds), Crime Spillover, *Sage Publications*, Beverly Hills, 7-19.

Herhalt, J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8:1-24

KPMG (2013). Global e Fr@ud Survey, KPMG Forensic and Litigation Services.

Kundi, G.M., Shah, B., & Nawaz, A. (2008). Digital Pakistan: Opportunities and challenges, JISTEM, Revista de Gestao da Technologia e Sistemas de

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

Informacao J*ournal of Information Systems and Technology Management*, Sao Polo, Brazil, 5(2): 365-390.

Kundi, GM. (2010). E-Business in Pakistan: Opportunities and Threats, Lap-Lambert *Academic Publishing*, Germany.

Lehman, D. (2000). Feds ID hacker who stole 485,000 credit-card numbers, Info World Daily News.

Leukfeldt, E.R (2014), "Cybercrime and social ties: Phishing in Amsterdam", Trends in Organized Crime.

Levi, M.(1998). Organized plastic fraud: Enterprise criminals and the side-stepping of fraud prevention, *The Howard Journal*, 37(4): 423-38.

Stuart F.H. Allison, Amie M. Schuck, Kim Michelle Lersch (2005). "Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics", *Journal of Criminal Justice*.

Johan Soderberg, Alessandro Delfanti (2015),"Hacking Hacked! The Life Cycles of Digital Innovation", Science, Technology, & Human Values.

Vol 4 (4) Oct-Dec,2018 pp.821-842.
ISSN 2520-7113 (Print), ISSN 2520-7121 (Online)
www.gjmsweb.com.editor@gjmsweb.com
Impact Factor value = 4.739 (SJIF).

CONTRIBUTION OF AUTHORS AND CONFLICT OF INTEREST

This research work was carried out in collaboration among three authors.

Author 1: Prof.Dr.Shaukat Malik has a Ph.D in Business Administration from Bahauddin Zakaria Multan He supervised the study and carried out statistical analysis.

Author 2, Shazia Noureen, is MS Scholar at Department of Business Administration, Institute of Southern Punjab. She designed the study, collected and analyzed data and prepared first draft of manuscript.

Author 3: Dr.Abdul Ghafoor Awan, is Ph.Ds in Economics from Islamia University of Bahawalpur-Pakistan and Business Administration from University of Sunderland, U.K. He contributed in this research paper by way of formatting, editing and giving final shape to the manuscript. All three authors read the manuscript carefully and declared no conflict of interest with any person or institution.