Vol 1 (Issue 2) April - June 2021, pp. 10 - 15

Cyber Crimes in Banking Sector - An Evaluation



Dr. A. Thilaha Dharmarajan
Assoc. Prof. - PG & Research Dept of Corporate Secretaryship
Bharathidasan Govt College for Women (Autonomous) - Puduchery
dratm71@rediffmail.com



U. Ezhilarasi
Research Scholar - PG & Research Dept of Corporate Secretaryship
Bharathidasan Govt College for Women (Autonomous) - Puduchery
ezhilarasiu14@gmail.com

E-banking is a boon of this century and a buzz word even to a layman with the introduction of Information Technology, with effect from October 17, 2000 which offered legal recognition to electronic transactions. The RBI is peeping into the legal compliance of online banking to guarantee monetary dependability. On the other hand, security threats play a predominant role in the Internet banking. As technology develops, Cybercrimes become the endangerment in the virtual world, people and organizations become the prey at an alarming rate as solely depending on web. Usage of internet and other technologies have enhanced the risk of attacks from cyber criminals across the globe. With the sharp rise of cybercrimes, banking sector is the hub in the occurrences of theft, phishing, PC infections, hacking and so on. In this scenario, there is an urge to investigate the security issues on the execution of technologies in banks and how to overcome such challenges is the need of the hour. In this study, the researcher makes an attempt to study the cybercrime scenario and its impact on banks in Puducherry.

Keywords: E-banking, Cyber - crime, Internet

1. Introduction

With the paradigm shift of Information Age, Computers have become the instrument through which criminal acts are carried out as Technology enabled crimes via internet. Net crimes are high-tech crimes as web connects people and devices across globally. As technology grows, security on money is also a question mark. Artificial Intelligence paves the way in fraud detection and banks should upgrade technology to combat cybercrimes. Banks rely on digital networking for their ample business scope. This in turn, aggravates the risk of banks and innocent customers to become victims of cybercrimes. Very common types of cybercrime include online bank data theft, identity theft, online predatory crimes and unauthorized computer access

2. Literature Review

In the words of Cybint, human error is the main cause of cyber security and 2020 was significantly

affected by online criminals and these will consistently go on in the coming years also.

A. Lakshmanan (2019) has done a study exclusively focused on cybercrime and found that cybercrime activities will be rising in the upcoming days and there is no full stop for that.

Ms. Neeta, Dr. V.K. Baksh (2019) have jointly published a research article on Cybercrimes in Banking Sector and suggested that cyber-attacks should be prevented by adhering strict compliance of law.

H. Singh Rao (2019) did a study to analyze Cyber Crimes in Banking Sector. The study highlighted the fact that India stands third among top 20 cybercrime victims.
In this scenario, the researcher attempts to study the cybercrimes which has major impact on banking sector. The study was made from the viewpoint of the Managers and Officers of Banks. The present study is unique in aspect and confines to Scheduled Commercial Banks in Puducherry alone.

3. Objectives of the Study

1. To identify the cybercrimes that affects the study area.
2. To examine the problems faced by banks in managing the cybercrimes and
3. To offer suggestions for the betterment of the study units.

4. Hypotheses

1. H01- There is no significant difference between a nature of bank and challenges faced by the banks for prevention of fraud.

2. H02- There is no significant relationship between gender and opinion of the bankers regarding Online banking which is better substitute for Traditional banking.

5. Methodology and Sample Design

There are 12 public sectors and 22 private sectors scheduled commercial banks in India, out of this 4 private banks viz., DCB Bank, Dhanalakshmi Bank Ltd, Jammu Kashmir Bank and Nainital Bank Ltd are not functioning in Puducherry. The researcher selected all 30 banks as the sample size and approached them for the study. All respondents responded except 3 private banks. Keeping in mind with the objectives set for the study, a sample size of 40 respondents are taken for the study by Census Sampling Method. Among the 44 questionnaires, only 40 respondents returned the filled in questionnaires. The sample of this study covers the Managers of the scheduled banks in Puducherry. Depend on the volume of business, market size and number of employees, the sample respondents has been chosen. Hence, the exact sample size of the study is 40.

6. Hypotheses

H01- There is no significant difference between a nature of bank and challenges faced by the banks for prevention of fraud.

H02- There is no significant relationship between gender and opinion of the bankers regarding Online banking which is better substitute for Traditional banking.

7. Results and Discussion

The results of the analysis of data are presented in the following pages.

Table 1: Cyber Crimes Detected by Banks

Sl.No	Cybercrime detected by banks	Responses		Percent of cases
		N	Percent	
1	Abuse of internet Access	5	10.20	16.10
2	Unauthorized access to information by insider	4	8.20	12.90
3	System penetration by outsider	2	4.10	6.50
4	Virus, Worm or Trojan infection	6	12.20	19.40
5	Website defacement	3	6.10	9.70
6	Computer facilitated financial fraud	1	2.00	3.20
7	Theft or breach of confidential Information	3	6.10	9.70
8	Hacking	2	4.10	6.50
9	Information forgery and counterfeiting	7	14.30	22.60
10	Denial of service	8	16.30	25.80
11	Electronic money laundering	3	6.10	9.70
12	All the above	3	6.10	9.70
13	Never	2	4.10	6.50
	Total	**49**	**100.00**	**158.10**

Source: Primary Data
Note: Multiple responses were obtained

The above Table portrays the Cyber-crimes detected by banks. It is evident from the study that the simple majority of the respondents 16.30% (8) responded Denial of service as the top most Cyber-crimes followed by Information forgery and counterfeiting 14.30% (7), Virus, Worm or Trojan infection by 12.20% (6), Abuse of internet access by 10.20% (5), Unauthorized access to information by insider by 8.20% (4), Electronic money laundering, Breach of confidential information and website defacement by 6.10% (3) each and the least by Computer facilitated financial fraud 2% (1). Hence, the major Cyber - crime detected by banks was Denial service.

Table 2: Challenges Faced by the Banks for the Prevention of Fraud

H01- There is no significant difference between a nature of bank and challenges faced by the banks for prevention of fraud

Nature of the Bank	Challenges faced by the banks for the prevention of fraud			
	Lack of customer and Staff Awareness	Difficult to integrate data to Various sources	Inadequate fraud detection tools and technologies	Total
Public Sector	10	5	9	24
Private Sector	5	2	9	16
Total	**15**	**7**	**18**	**40**

Source: Primary Data.

Chi-Square Tests

	Value	DF	Asymp.Sig.(2 -Sided)
Pearson Chi-Square	1.409[a]	2	0.494
N of Valid Cases	40		

Source: Primary Data

It is highlighted from the Table.2 that the chi-square value is 1.409 which is greater than the T able value 0.494. Hence the hypothesis is rejected. Therefore, it is concluded that there is significant variation between nature of bank and challenges faced by the bank for the prevention of fraud.

Table 3: Online Banking is Better Substitute for Traditional Banking

H02- There is no significant relationship between gender and opinion of the bankers regarding Online banking which is better substitute for Traditional banking.

Gender	Online banking is better substitute for traditional banking		
	Yes	No	Total
Male	21	2	23
Female	17	0	17
Total	**38**	**2**	**40**

	Value	DF	Asymp.Sig.(2 -Sided)
Pearson Chi-Square	1.556[a]	1	0.212
N of Valid Cases	40		

Source: Primary Data

It is evident from Table 3 that the chi-square value is 1.556 which is greater than the table value 0.212. Hence the hypothesis is rejected. Therefore, it is concluded that there is significant relationship between gender and opinions of the banker regarding online banking is better substitute for traditional banking.

Most of the respondents responded that Fraud control strategies and policies should be improved, as well as Employee code of conduct should be developed to tackle the fraud.

8. Findings of the Study

1. There is no positive association between nature of banks and customer using e-banking services.

2. Very few 12.5% (5) respondents ‘strongly agree’ to the protective measures regarding termination of online transaction completely.

3. It is observed that the 50% of the respondents are strongly Agree with the protective measures on backup of important data.

4. It is found that 52.5% of the respondents are strongly agreed for use security programs to safeguard the important data.

5. The major Cyber- crime detected by banks was Denial service.

6. There is significant variation between nature of bank and challenges faced by the bank for the prevention of fraud.
.
7. There is significant relationship between gender and opinions of the banker regarding online banking is better substitute for traditional banking.

9. Suggestions

1. Though security measures are taken by the bank, lot more to keep the customer account safe. It is suggested to hire employee with strongly IT Background with proper training, skill and updated knowledge.

2. It is suggested that all transactions have two steps authentication to keep the customers' accounts in safety aspect. It is necessary to have an update Anti-virus software to safeguard against virus attacks should be used and also to keep a backup so as to avoid data loss in case of virus threat.

3. It is further suggested to the bank to conduct training and orientation programs for the bank employees. The employers should be made mindful about fraud anticipation measures. It very well may be done through bulletins or magazines illuminating cheats related parts of banks by senior functionaries, setting up 'Rules and regulations in the work environment of the representatives, security tips being streaked on screen at the hour of signing into Core Banking arrangement programming, having conversations on factors causing cybercrime and activities needed to be embraced in taking care of them. -

4. Employees who go beyond their call of duty to prevent cyber frauds if rewarded will also enhance the work dedication. Bank frauds also shows that customers engage in internet banking are not alert and not have sufficient knowledge on cyber threats. It is the duty and responsibility of banks to aware and educates the customers time to time about prevailing threats in the market. The study has proved that lack of preparedness is one of the reasons for cybercrime. Hence, it is high time, suggested for both banks and customers in the adoptions of new technological changes.

10. Conclusion

The rapid growth of technology requires banks to review their policies and make their system stronger. Banks can aware customers through their websites about banking frauds and what measures should be taken to prevent these crimes. Banks ought to have review advisory group to regulate the false and fraud activities in banks. They should take sufficient measures to combat these crimes and hire employees with strong IT background with proper training, skill and updated knowledge. Together, banks and customers win the race for better tomorrow.

References

1. https://www.varonis.com/blog/cybersecurity-statistics

2. Business Line, 7th December 2020

3. Lakshmanan A (2019) “Literature review on Cyber Crimes and its Prevention Mechanisms” UniversitiSains Malaysia, pp.01-05.

4. Neeta, Dr.V.K.Bakshi, (2019) “Cyber Crimes in Banking Sector”Aayushi International Interdisciplinary Research Journal (AIIRJ), Vol.VI, Issue V, pp.25-31.

5. Singh Rao(2019), “Cyber Crime in Banking Sector”, International Journal of Research -Granthaalayah, 7(1), pp.148-161.