42

A Systematic Study into Cyber Security Issues Facing Indian Banks

*Dr. Kamal Kant**

Abstract

The Indian government declared the country's demonetarization on November 8, 2016. Online banking and transactions have completely changed essential activities in the twenty-first century. The public uses internet transactions extensively and experiences cybercrimes. Cybercriminals commit cybercrimes such borrowing money, obtaining credit, hacking, and so forth. Hacking into unauthorized systems and obtaining personal data is considered cybercrime. Several crucial techniques are offered here to protect against cyber attacks.

Keywords: Cyber security, digital payment, cyber-attacks.

INTRODUCTION

A constantly changing collection of obstacles confront the global financial scene, including as operational weaknesses, market volatility, geopolitical unpredictabilities, cyber security concerns, and worries about regulatory compliance and debt levels. In differing degrees, these risks carry the potential to set off financial crises, cause market disruptions, and affect global economic growth. Financial institutions, regulators, and market participants need to be alert and flexible in this changing climate. In order to handle and mitigate these hazards, effective risk management, regulatory monitoring, technology innovation, and international cooperation are essential elements.

Right now, cyber security poses an increasing concern to all firms. Specifically, in the last year, it has become abundantly clear that the banking industry has several vulnerabilities in its infrastructure and cyber security protection.

*Department of Business Administration, Faculty of Commerce and Management Studies, Jai Narain Vyas University, Jodhpur (Rajasthan.)

Since hackers have been breaking into people's, businesses', and governments' bank accounts and demanding large ransoms to unlock force-encrypted data, these attacks have become extremely targeted.

Review of Literature

Claessens et al., (2002) the banking industry has seen a number of frauds and cybercrimes, including debit card fraud, cyber money laundering, and ATM fraud. Nonetheless, the main objective of all frauds is often to enter the victim's bank account, take money, and transfer it to another bank account..

Moore.T, Clayton.R&Anderson.R (2009) centered on the topic of cybercrime. The majority of online crimes are the result of bothersome hacking by inexperienced hackers. This article examines numerous issues and facts related to cybercrime issues that banks and law enforcement agencies have in managing traditional law enforcement. The paper's analysis demonstrates that there is room for considerable advancements in the way that online fraud is handled, and that understanding the economics of online crime is a recommended first step in researching it.

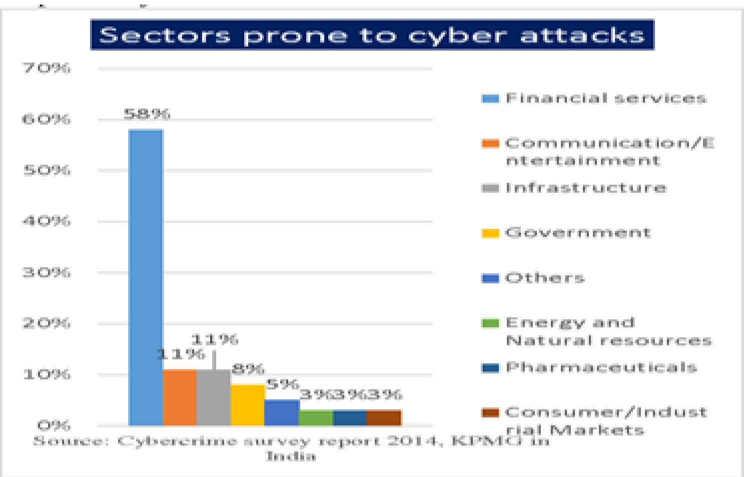
Florêncio&Herley, (2011) given the numerous weaknesses in the banking industry's defense system, it is necessary to look into strategies to raise public knowledge of the steps that may be taken to prevent cybercrimes in this industry. Nevertheless, there haven't been many researches done in this field in the past that may offer recommendations for reducing the dangers and stopping such crimes.

Objectives of the Paper

To research the various types of cybercrimes related to online transactions.

- To explore current online banking security systems;
- To Examine difficulties related to cyber security in digital transactions;
- To evaluate potential solutions to the threat of cyber security in online banking.

Cybercrime

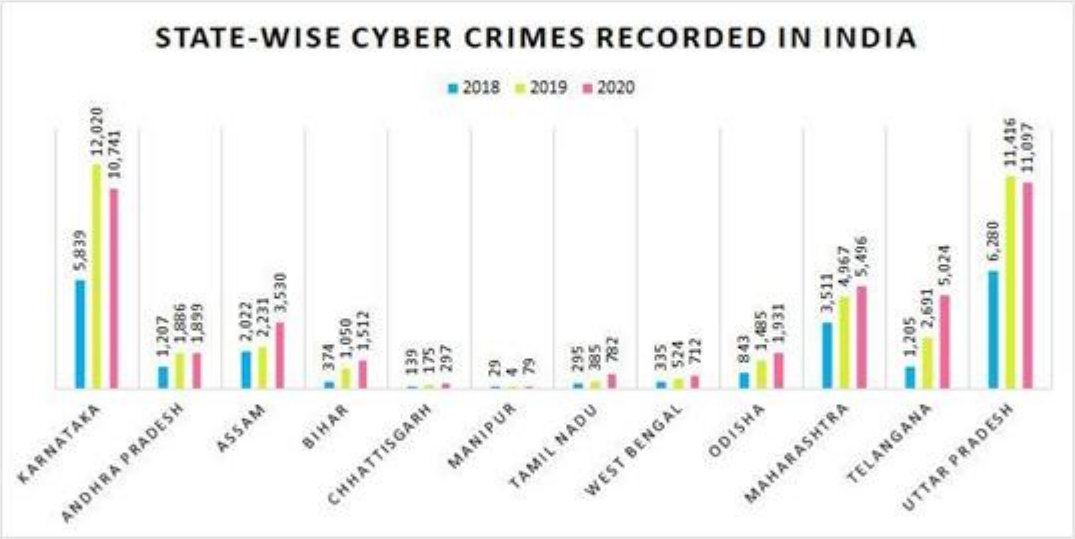


Source: Cybercrime survey report 2014, KPMG in India

One of the fundamental elements that dictate a nation's progress and expansion is its economy. The banking industry is thought to be the foundation of the economy. We carry out our daily operations using demand drafts, checks, and cash. On the other hand, this design has made room for a new credit/debit card-swiping payment method. In its 1991–1998 report on financial concerns, the Narasimha Committee recommended that information technology (IT) be employed to improve the efficiency of the banking industry.

This study's goal is to examine the underlying strategies used to highlight the concerns regarding cyber dangers to the banking industry. It focuses on how prepared financial institutions are to handle incidents of cybercrime.

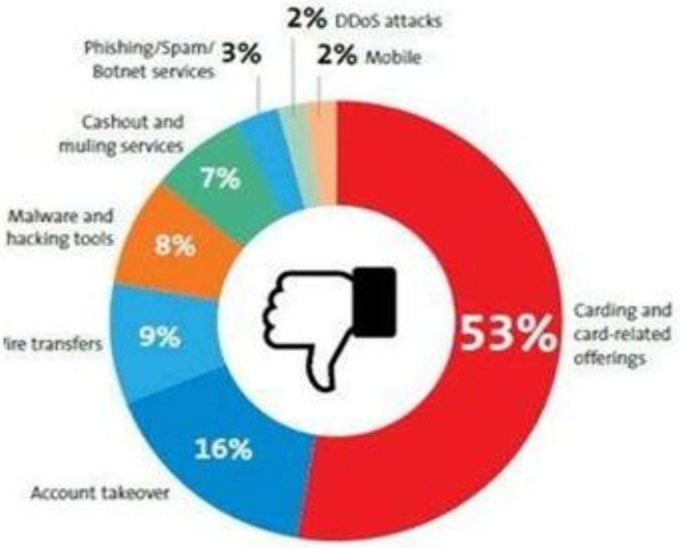
Cyber Crime in Banking Industry



Cybercrime is any illegal activity that takes place online or through a computer. To put it another way, digital misconduct is also known as cybercrime, when a criminal uses a computer or any other electronic device and the internet to commit a variety of crimes, including money transfers and withdrawals through unauthorized access.

In conclusion, in today's globalized world, the banking industry offers a wide range of services to its customers with including credit card services and internet banking.. "Paying online with a debit card" Consumers have round-the-clock access to all bank services, and they can use their phones and the internet to conveniently conduct business and manage their accounts from any location in the world." Although these services are helpful to users, as we all know, they also have a negative aspect that includes robberies and hackers.

Cybercrime Types Associated with the Banking Sector



6.1 HACKING

Hacking is a type of cybercrime where an individual attempts to breach security measures by breaking into banking websites or customer accounts, or they gain unauthorized access to a system..

6.2 VIRUSES

It is a type of self-replicating software that inserts copies of itself into documents or executable code to infect them. An executable file that has been infected by a program that makes it behave strangely is called a virus. It propagates by attaching itself to executable files, including operating systems and program files. The executable file loading process may cause the virus to replicate itself. Worms, on the other hand, are programs that have the ability to copy themselves from the victim's computer and send copies to other computers. Worms replicate and transfer copies of themselves from the user's computer to other computers without altering or deleting any files.

6.3 SPYWARE

The most popular method for taking online banking credentials and using them fraudulently is spyware. Information is gathered or sent between computers and websites by spyware. Most often, it is installed by false "pop up" adverts that request that software be downloaded. This kind of software is found and eliminated by industry-standard antivirus programs, mostly by preventing the download and installation of the program before it infects the computer.

6.4 PHISHING

Phishing is a type of scam where emails that appear to be from reputable sources are used to steal personal information such as customer ID, IPIN, CVV number, debit/credit card number, and expiration date. Email spoofing and instant messaging are two methods used in phishing.

In this kind of fraud, con artists pose as bank employees and create a direct link that takes the intended victim's browser to a phony webpage that mimics the real bank website. On the customer's account, fraudulent transactions are subsequently carried out using the obtained confidential information.These days, phishers also use mobile (voice phishing) and SMS (smashing) techniques to carry out their crimes.

6.5 PHARMING

The internet is used for pharmacological operations. The hackers manipulate the URL so that when a consumer visits a bank's website, they are taken to a fake website that imitates the bank's original one.

6.6 ATMSKIMMIN GAND POINT OF SALE CRIMES

Installing a skimming device on top of the machine keypad to make it appear like a real keypad or a device linked to the card reader to make it appear like it is a component of the machine is one way to get into ATMs or point-of-sale (POS) systems. Malware that directly steals credit card information may also be installed on these devices. Card numbers and personal identification numbers (PINs) can be obtained from ATMs that have skimmers installed successfully. These details are then copied and utilized in fraudulent transactions.

6.7 DNSCACHEPOISONING

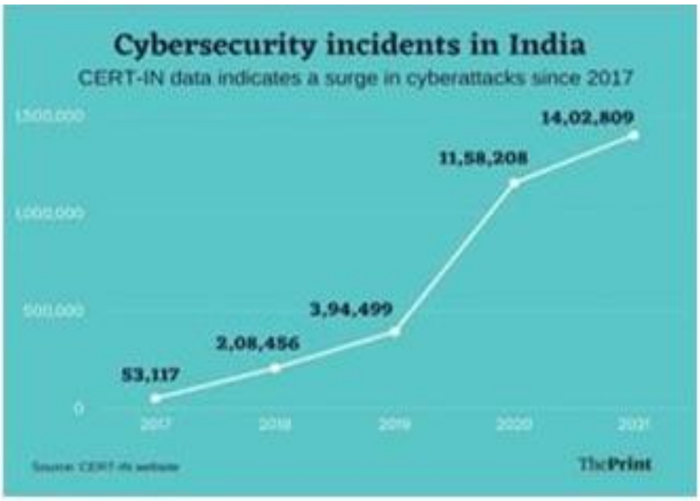
In an organization's network, DNS servers are used to speed up resolution response times by storing previously received query results in cache. By taking advantage of a vulnerability in DNS software, poisoning attacks against DNS servers are executed. The server will serve incorrect entries to all users who make the same request from its local cache. Bank clients may be redirected to a criminal-controlled server, where malware may be served up or they may be tricked into entering their login information for a fraudulent website. IP spoofing is a technique used to gain control over clients. It involves changing DNS records for a bank's website from one DNS server to another, using the IP address of a server they own.

Cybercrime's Influence on Banks

The proliferation of mobile networks in daily life and the advancement of information and technology (IT) have made financial services more accessible to a wider audience. But while technological advancements have made banking services more accessible and affordable, they have also increased the risk of becoming a target of cyber-attacks.

The ingenious methods used by cybercriminals to steal money, spy on companies, and access private company information have an indirect effect on the bank's finances. To counteract these cybercrimes, the banking industry must work with government authorities and watchdog groups to build a control paradigm..

The primary area of interest in this case is the dearth of an effective compilation service in the banking sector that is capable of identifying cybercrime patterns and building a model around them.



A. Cyber-Attacks in India

1. Cosmos Bank Cyber Attack in Pune

2018 saw hackers steal Rs. 94.42 crores from the Pune-based bank Cosmos Cooperative Bank Ltd. India's banking industry was shaken by the hack. This cyber attack was directed on Cosmos Bank. Hackers gained access to the bank's ATM server and stole a substantial quantity of personal data belonging to Visa and Rupee debit cardholders. After learning that money had been destroyed, cyber groups from as many as 28 nations immediately withdrew the monies. It can be avoided by bolstering surveillance procedures and assisting those who are permitted.

2. ATM System Acked

A hack was conducted in 2018 against Canara Bank's ATM servers. Twenty lakh rupees were taken out of many bank accounts. Cybercriminals allegedly had access to the ATM credentials of over 300 individuals, creating a total of 50 victims. Hackers used devices known as skimming devices to collect debit cardholder data. The stolen data was used in transactions totaling between Rs. 10,000 and Rs. 40,000. It can be avoided if ATM security measures are reinforced to stop data misuse.

3. The Bank NSP Case

In one case, a bank management trainee was engaged to be married. The two made extensive use of the company's computers to send and receive emails. They separated after a while, and the girl started making up fake email accounts, such as "Indian bar associations," to communicate with the boy's international customers. She did this on the computer at the bank. The boy's company lost a lot of business, so it filed a lawsuit against the bank. The bank was found liable by the court since the emails were sent using the bank's system.

B. Techniques for Stopping Cyber Crime

1. Every worker should have a user account, and it should be mandatory to update passwords every three months according to policy. It is imperative that unapproved software cannot be downloaded or installed by employees.
2. Every employee needs to be made aware of the risks involved in downloading or opening email attachments from unknown senders. Inform staff members of the significance of not disclosing or exchanging private information about the organization.

3. A bank's IT department needs to make sure that every workstation and device linked to the Internet has a firewall turned on since they prevent any communication from entering the system from unapproved sources.
4. Anti-spyware and anti-virus software needs to be installed on every PC in order to detect the presence of ransomware or dangerous malware on the network. Wireless networks and all passwords need to be kept safe and secure.
5. With increasing customers using mobile devices, banks need to deploy verification techniques such web-based transaction verification and dynamic device authentication.
6. Banks are required to send automated messages and notifications to their customers verifying the legitimacy of their transactions.

Conclusion

Indian consumers are favoring online services more and more because of their great ease of use, cost-effectiveness, and speed of transactions. Furthermore, with lower operating costs, financial institutions are hoping to increase the number of cashless transactions by offering consumers exciting deals. That being said, this suggests that a dynamic technological environment and improved attacker skills are surpassing economic institutions' cyber security initiatives to combat cybercrime. The increasing prevalence of cybercrime makes it evident that local law enforcement agencies do not have the necessary resources or expertise to look into incidents involving cybercrime. In order to get faster and more accurate results from cybercrime investigations, it is better to use trained cyber security experts.

References

[1] Acharya, Suman, and Sujata Joshi. "Impact of cyber Attacks on banking institutions in India: A study with special of safety mechanisms and preventive measures." PalArch's Journal of Archaeology of Egypt/Egyptology 17.6 (2020): 4656-4670.

[2] Deborah Golden and IrfanSaif, ―The future of cyber survey 2019‖, Deloitte, 2019, https://www2.deloitte.com/us/en/pages/advis ory/articles/ future-of-cyber-survey.html

[3] M Sravika, A Study on Cyber Security Issue Affecting Banking and Online Transactions, Sridevi Women‗s Engineering Collaege. Jan-2022

[4] R.P.Kaur, (2013) Statistics Of Cyber Crime In India: An Overview‖, International Journal of Engineering and Computer Science, vol.2, no. 8, pp. 2555-2559.