International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/intjecse/v14i5.1177 ISSN: 1308-5581 Vol 14, Issue 05 2022

CYBER CRIMES IN BANKING SECTORS: AN OVERVIEW

Mahesh Pratap Singh Shekhawat[1]
Dr.Priyanka Joshi[2]

ABSTRACT
Cybercrime refers to the use of a computer to advance illicit activities like fraud, the trafficking of child pornographic material and other intellectual property, identity theft, privacy invasions, etc. It entails spreading viruses, downloading files unlawfully, engaging in phishing schemes, and stealing personal data like bank account numbers, etc. Thus, a crime can be identified as a "cybercrime" if "computer" and "internet" are among its primary components. Because of this, computer crimes are frequently used to refer to cybercrimes. The majority of cyberattacks fall under the category of "economic crimes," which are typically carried out by highly organized criminals and employ the most cutting-edge technologies.The number of cases of financial fraud has risen along with the rate of innovation. Different methods are being used by cybercriminals to gather bank information and conceal their funds. The banks have employed a number of specific procedures to protect against these frauds, yet the problem persists. This is explained by the fact that the security measures currently available through banks are also available in public or in other places where they can be exploited by cybercriminals who can simply breach security measures.Banking sector has suffered an impact of cybercrimes. RBI has defined bank fraud has as, "A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank."
KEYWORDS: Cyber Crime, Banking frauds, IT Industry,Hacking, Spyware, Credit card fraud, Virus, Narasimha Committee

INTRODUCTION
Cyber-crimes in the 21st Century has emerged to be one of the most lethal revengeful weapons that any person can use to threaten or cheat someone. The active internet users as per the latest reports of January 2021, were around 4.66 billion and this growth has led to the increase in the chances of a user being trapped in this malicious method of crimes which has been in surge during the past few decades. Although it is understandable that computers have become an essential part of one's existence, they have also developed an environment conducive to cyber-crime. Cyber-crimes pose a major challenge in light of the fast-changing environment and the significant contribution of the IT industry. Cybercrime is typically carried out by offenders who have technological skills who can outstrip and think one step ahead of the law in order to gain access to computers and commit crimes.

The economy is among the foundations that determines a country's development and growth. The banking sector is regarded as the economy's backbone. We use cash, cheques, and demand draughts to conduct our daily business. This pattern, however, has paved the way for a new payment system based on swiping debit or credit cards. The Narasimha Committee (1991-1998) which was for the recommendation on financial matters, suggested that IT shall be used in the banking sector as well to make it more efficient in the functioning.

While the banking sector has expanded its services and aims to provide excellent customer service via innovation, cyber-crime continues to be a problem. Cyber criminals can easily get in touch that is accessible on the internet. Cyber-crime causes massive monetary losses, that are borne not only by customers, but also by banks, affecting a country's economy. When viruses are produced and spread on other devices, or when sensitive business information is posted on the Internet, non-monetary cybercrime exists. Phishing and pharming are the most popular examples.

Due to enhanced online recognition through alternative platforms such as the internet, ATMs, and mobile banking, India has seen an increase in the amount of debit/credit cards. This amount will gain momentum in the coming days as the young generations enters the financial tumult. The objective of

[1] Research Scholar, Apex School of Law, Apex University, Jaipur (Rajasthan)-303002
[2] Supervisor, Apex School of Law, Apex University, Jaipur (Rajasthan)-303002

this study is to scrutinize the concerns about cyber threats to the banking sector by highlighting the underlying tactics. It focuses on how well financial institutions are equipped to deal with cyber-crime events.

CYBER CRIME IN BANKING INDUSTRY

Cybercrime refers to any criminal activity carried out on a computer or over the internet. In other words, digital misconduct is referred to as cybercrime where the criminal exercises a number of wrongdoings such as money transfers and withdrawals via unauthorized access by using the computer or any other electronic devices and the internet.

To narrow down the landscape in today's globalised world, the banking industry offers many services to their clients and consumers, such as online banking and credit card services. "Online payment with a debit card Customers can access all types of bank facilities 24 hours a day, and they can conveniently transact and run their accounts from anywhere in the world using the internet and cell phones. “As we all know, these services are useful to customers, but they also have a dark side, which includes hackers and robberies.

They take advantage of those services by breaking into banking websites and customers' accounts, causing chaos in accounts and theft of money from customers' accounts, the best example was "in which one hacker took one rupee from each account but received a large sum of money with that one rupee."

EFFECTS OF CYBER CRIMES

Cybercrime may have long-term consequences on those who are attacked. Cyber attackers carry out cyber threats such as taking out loans, incurring credit, hacking, and so on, which may have devastating effects in the banking business.

The below are the effects:

i. Financial loss
ii. Infringement of confidential information
iii. Legal consequences
iv. Sabotage and theft to identifiable information
v. Exposed to reputation risks
vi. Operational risks

REASONS FOR CYBER CRIMES

Easy access to data

Once a cyber attacker is able to gain access into a computer system, they may have access to personal data, including private financial documents from customers, which can be copied or transferred into a small removable device. Since information technology powers the operations of banks, individuals, corporations, government agencies, etc., the insecure storing of confidential data and information processed on their computers presents a serious danger.

User's Negligence

All the authorities who use computer systems should remain very careful and cautious in order to safeguard their confidential data and information stored in the computers. Through proper usage of Passwords and Personal Identification Numbers (PIN) they can limit the access. Any negligence on their part will facilitate cybercriminals' easy access to certain devices and records.

Lack of internal control in organizations and banks

Banks use a variety of operating systems for their day-to-day activities; hence banks must ensure that they have in place ongoing internal control and IT audit systems otherwise it can result in computerized environment lapses due to the availability of inefficient software and hardware systems.

TYPES OF CYBERCRIMES CONNECTED WITH BANKING SECTOR

Hacking

Hacking is a cybercrime that involves a person gaining illegal access to a system or attempting to circumvent security mechanisms by hacking into customers' accounts or banking sites. "A hacker, however, can be prosecuted under Sections 379 and 406, and also u/s 43(a) read with Section 66 of the Information Technology (Amendment) Act, 2008." If the crime of hacking is proven, the convicted may be sentenced to three years in prison or a fine of up to five lakh rupees, or both, under the IT Act.

Key logging

It is referred to as "keystroke logging or keyboard capturing". It is the process of secretly recording (logging) the keys pressed on a keyboard so that the person using it is oblivious that their activities are being tracked and these are incredibly harmful for stealing confidential information such as banking details etc.

Viruses

It is a kind of self-replicating program that infects executable code or documents by inserting copies of itself. A virus is a programme that afflicts an executable file and causes the file to behave abnormally after infection. It spreads by linking itself to executable files such as programme files and operating systems. Loading the executable file could result in new copies of the virus being created. Worms, on the other hand, are programmes that can replicate themselves and send copies to other computers from the victim's computer. Worms do not change or remove any files; instead, they multiply and send copies to other computers from the user's computer.

Spyware

Spyware is the most common approach of stealing online banking credentials and using them for fraudulent purposes. Spyware operates by collecting or transmitting information between computers and websites. It is mostly installed by bogus 'pop up' advertisements to have software downloaded.Industry standard Antivirus products detects and removes this type of software, primarily by blocking the download and installation before it infects the PC.

Phishing

Phishing is a kind of swindle in which private information such as Debit/Credit Card number Customer ID, IPIN, CVV number, Card expiry date, and so on is stolen via emails that seem to be from a genuine source. Phishing is accomplished through the use of instant messaging and email spoofing.

In this type of crime, hoaxers act like officials of banks and they create a direct link that directs the targeted customers to a fake page which looks alike to the actual bank website. The acquired confidential information is then used to commit deceitful transactions on the customer's account. Phishers these days also use SMS (Smishing) and mobile (voice phishing) to commit such crimes.

Pharming

Pharming is carried out through the internet. When a customer logs in to a bank's website, the attackers hijack the URL in such a way that they are routed to another website that is false but appears like the bank's original website.

ATM Skimming and Point of Sale Crimes

Installing a skimming device atop the machine keypad to appear as a real keypad or a device made to be affixed to the card reader to appear as a part of the machine is a tactic for compromising ATM machines or POS systems. Malware that directly steals credit card data may also be installed on these devices. Skimmers that are successfully installed in ATM machines retrieve personal identification number (PIN) codes and card numbers, which are then copied to perform deceitful transactions.

DNS Cache Poisoning

DNS servers are used in a company's network to increase resolution response times by caching query results previously received. Poisoning attacks on DNS servers are carried out by exploiting a flaw in DNS software. As a result, the server validates DNS responses mistakenly to ensure that they are from an authoritative source. Incorrect entries will be cached locally by the server and served to all users who make the same request. Bank customers could be routed to a server controlled by criminals, which could be used to serve malware or trick bank customers into providing their credentials to a spoof of a legitimate website. An attacker can hijack clients by spoofing an IP address; DNS entries for a bank website on a given DNS server and replacing them with the IP address of a server they control.

Malware based-attacks

One of the most dangerous cyber threats to electronic banking services is malware-based attacks. A malicious code is created in such attacks. The number of malware attacks in the banking industry is on the rise these days. Zeus, Spyeye, Carbep, KINS, and Tinba, are some of the most well-known banking malwares. Nearly every virus has two characteristics: one, it secures a backdoor entry into the system, and the other, it steals a user's credential information.

IMPACT OF CYBERCRIME ON BANKS

Due to geopolitical and global macroeconomic conditions, the banking industry in the world is facing a difficult situation that is thought-provoking. In order to better analyse and mitigate risks, the banking industry is being forced to review its existing practices. For risk management, technology-driven approaches have been used.

Financial services have been expanded to the masses as a result of the development of information and technology (IT), as well as the penetration of mobile networks in daily life. However, technology advancement has made the banking services accessible and affordable but this in turn has augmented the likelihood of being a target of cyber-attacks.

Cyber thieves have developed sophisticated methods to not only steal money, but also to spy companies and gain access to vital business information, which has an indirect effect on the bank's finances. To combat such cybercrimes, the banking industry must work with national authorities and watchdog organizations to create a model that will aid in control.

The major source of interest here is the lack of an efficient compilation service in the banking industry that can detect patterns in cybercrime and compile a model based on them.

CYBER-ATTACKS IN INDIA

Cosmos Bank Cyber Attack in Pune

Cosmos Bank in Pune was the target of a recent cyber-attack in India in 2018, when hackers stole Rs. 94.42 crores from Cosmos Cooperative Bank Ltd situated in Pune, it rattled the entire banking industry in India. Hackers gained access to the bank's ATM server and stole the personal information of rupee debit cardholders and visas in large number. Money was wiped out, and hacker gangs from as many as 28 nations withdrew the funds as soon as they were notified. It can be avoided by hardening surveillance measures and assisting approved individuals.

ATM System Hacked

The ATM servers of Canara Bank was targeted in 2018 for cyber-attack. Twenty lakh rupees were cleared from numerous bank accounts. According to sources, cyber criminals had access to ATM information for more than 300 users, resulting in an overall 50 victims. Hackers used skimming machines to capture information from debit cardholders. Transactions involving stolen information varied in amount from Rs. 10,000 to Rs. 40,000. It can be avoided if the protection mechanisms in ATMs can be improved to avoid data misuse.

RBI Phishing Scam

The Reserve Bank of India was not spared by the fraudsters in a bold phishing attempt of its kind. The phishing email, which purported to come from the RBI, promised the recipient prize money of Rs.10 lakhs within 48 hours if they clicked on a connection that took them to a website that looked exactly like the RBI's official website, complete with the same logo and web address. After that, the user is asked to disclose personal details such as his password, I-pin, and savings account number. The RBI, on the other hand, issued an alert about the fake phishing e-mail on its official website.

The Bank NSP Case

In this particular case a bank management trainee was hitched to be married. Using the company's computers, the couple exchanged numerous emails. They had broken up their marriage after some time, and the young lady made some fake email ids, such as "Indian bar associations," and used them to send emails to the boy's international clients. She did this via banks computer. The boy's business lost a large number of customers and went to court against the bank. The court decided and made the bank liable because the emails were sent using the banks system. The aforementioned cyber-attacks in India should act as an alert to all individuals and companies who are already prone to cyber threats. It is crucial for the banking industry and organizations to adopt cyber security measures and adhere to security guidelines.

Methods to prevent cybercrime

The crimes in the banking industry have alarmingly increased which have resulted in significant economic losses. As we all know that banking is the most important mainstay of our economy, so it must be prevented from cyber-attacks. Awareness should be made to the banks and the customers regarding the risk involved and also the safety measures to combat the cyber-attack.

For the effective implementation of all the matters of cyber security policy, the government has established an "Inter-Departmental Information Security Task Force (ISTF)" with the National Security Council as the nodal agency. The national nodal agency is the "Indian Computer Emergency Response Team (CERT-In)" which is entrusted to check the computer security incidents as they happen.

The main problem related with cybercrime is jurisdiction. Cybercrime happens in every state so any person, regardless of where they live, should be able to recognise and monitor cybercrimes. In certain cases, victims of cybercrime may be impotent to report a cybercrime for a variety of reasons, like living in a distant area, being unsure of where to report, and privacy concerns. As a result of the nonexistence of a centralized online cybercrime monitoring system, many cybercrime incidents go unreported.

The IT Act should be revised to include a definition of cybercrime as well as a list of instances in which the Act would have extraterritorial authority. The scope of the IT Act should be expanded to include the legislative basis for cyber regulation in India. The intermediaries' responsibilities are ambiguous but that should me made explicit.

NUMEROUS WAYS TO REDUCE THE DANGER OF CYBER-ATTACK

1. Every single employee should have their own user account, with a policy requiring password changes in every three months. Employees must not be allowed to download or install unauthorized software.
2. All employees must be informed about the dangers of opening or uploading email attachments from unidentified sources. Educate personnel about the importance of not leaking or sharing sensitive information about the institute.
3. The IT department of a bank must ensure that a firewall is enabled on every workstation and Internet-connected device in the organization because firewall blocks all communication from unauthorized sources.
4. Banks must use 'two-factor authentication (2FA)' apps or physical security keys and, wherever possible, enable 2FA on all online accounts.
5. The Department would make sure that all PCs' operating systems receive regular security updates.
6. To find out if there is any ransomware or malicious software on the network, anti-spyware and anti-virus software must be installed on all PCs. All passwords and wireless networks must be kept secured and well-protected.
7. Banks must employ verification methods such as dynamic device authentication and web-based transaction verification as more consumers use mobile devices.
8. Customers must receive notifications and automated messages from their banks confirming the validity of their transactions.
9. Customers must be given instructions on how to verify the legitimacy of any sources that are asking information of personal accounts. Customers must also be given instructions on how to stay safe when using the bank's websites.
10. When using banking application or internet banking, use a secure network.

CONCLUSION

Due to the extreme ease, cost savings, and speed of online transactions, Indian consumers are increasingly preferring online services. Furthermore, financial institutions are presenting consumers with exciting deals in the hopes of increasing the number of cashless transactions due to lower operating costs. That being said, this can be indicated that economic institutions' cyber security initiatives to combat cybercrime are being outpaced by a dynamic technical environment and increased attacker skills.

The financial system's backbone has been information technology. It supports the growing difficulties and banking requirements tremendously. Currently, banks cannot consider introducing financial products in the absence of Information Technology. Information Technology, on the other hand, has had a negative effect on our financial industry, where crimes such as stealing, hacking, phishing and forgery are perpetrated.

When an individual engages in any type of electronic banking transaction, it is necessary to ensure authentication, identification, and verification techniques to deter cybercrime. The rise of cybercrime and the sophistication of the investigative process necessitates the adoption of adequate steps. In order to combat cybercrime, it is important to improve stakeholder collaboration. As part of their overall operational risk management mechanism, banks must keep up with the latest changes in the IT Act, 2000, and the orders, laws, notices and regulations issued thereunder relating to bank transactions, as well as embryonic legal requirements on electronic fund transfers, electronic signatures, data security, digital signatures and cheque truncation. During the continual improvement of the technologies used at the financial institution's backend, certain critical aspects were ignored, which now require immediate attention. Cybercrime has its own range of appealing characteristics that have increasingly begun to overshadow conventional crimes. Cybercriminals are attracted to the level of anonymity, global victim reach, and quick outcomes, to name a few. Cyber criminals' job is made easier by the lack of/inadequate awareness campaigns. Owing to a lack of knowledge about the most recent attack methodologies and documented preventive steps, unaware customers are easily fooled. With the growing influence of cybercrime, it is becoming increasingly clear that local law enforcement agencies lack the requisite skills and resources to investigate incidents involving cybercrime. Using trained cyber security experts takes it a step further in terms of obtaining faster and more accurate cybercrime investigation results. It is believed that after ensuring and estimating upon the proper checks on all the problems and involving all the stakeholders to solve this major problems relating to the technological growth in the developing countries like India, these kind of risks as mentioned in the research work can be minimised to a certain extent and we can in a way ensure India to be digitally safe and secure.

REFERENCES

- Joseph Johnson, Worldwide digital population as of January 2021 (Statista, 7 Apr 2021)
- A.R. Raghavan and Latha Parthiban, The Effect of Cybercrime on a Bank's Finances (2014) 2(2) International Journal Current Research Academic Review 173-178.
- Harshita Singh Rao, Cyber Crime in Banking Sector (2019) 7(1) International Journal of Research Granthaalayah 148-161
- Effects of Cyber Crime
- Kate Brush, Cybercrime (Search Security)
- Indian Penal Code 1860, s 379 & 406.
- Information Technology (Amendment) Act 2008, s 43(a) r/w s 66.
- Seema Goel, Cyber-Crime: A Growing Threat To Indian Banking Sector [2016] ICRISTME.
- Stay Safe from these Credit Card Frauds (Axis Bank, 1 January 2021)< https://www.axisbank.com/progress-with-us/managing-credit/what-are-the-types-of-credit-card-frauds-in-india#:~:text=Steps%20to%20take%20if%20card%20is%20stolen%3A&text=Immediately%20block%20your%20card%20using,%2Dliability'%20for%20fraudulent%20transactions> accessed 7 March 2021.
- Vivek Kumar Verma, Phishing (Indian Case Law, 16 July 2014) < https://indiancaselaw.in/phishing/
- AnimeshSarmah, RoshmiSarmah , Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Laws of India (2017) 4(6) IRJET 1634.
- Robert Siciliano, ATM Skimming and How to Protect Yourself(The Balance, 9 August 2020) https://www.thebalance.com/what-is-atm-skimming-1947475
- What are DNS Spoofing, DNS Hijacking, and DNS Cache Poisoning (Infoblox) https://www.infoblox.com/dns-security-resource-center/what-are-dns-spoofing-dns-hijacking-dns-cache-poisoning
- Express News Service, Cosmos Bank Malware Attack: Interpol Issues Red Corner Notice Against Prime Suspect Traced in Foreign Country Indian Express (Pune, 29 August 2020) https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-interpol-issues-red-corner-notice-against-prime-suspect-traced-in-foreign-country-6574097
- Ranjitha S, 4 Biggest Cyber Security Threats for Indian Banking Sector (Great Learning, 24 March 2021) https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-

banking-sector/#:~:text=Canara%20Bank%20ATM%20servers%20were,rupees%20from%20various%20bank%20accounts

- Vivek Kumar Verma, Phishing (Indian Case Law, 16 July 2014) < https://indiancaselaw.in/phishing
- Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Laws of India (2017) 4(6) IRJET 1636.
- Harshita Singh Rao, Cyber Crime in Banking Sector (2019) 7(1) International Journal of Research Granthaalayah 158 accessed 11 March 2021.
- How the Banking Sector Can Combat Cyber Attacks: A Checklist (Byte Academy, 6 August 2020) https://www.byteacademy.co/blog/banking-cyber-security.