CYBERCRIME AN EMERGING CHALLENGE IN BANKING SECTORS: AN OVERVIEW

By Akansha Upreti
From Amity Law School, Noida

Abstract:

With the headways in innovation, the banking industry has enjoyed the ride of emerging technology to undergo significant variations. Banks are among the biggest beneficiaries of the IT (Information Technology) revolution and have largely adopted IT solutions for rendering the banking services to their customers. The propagation in online transactions mounting on technologies like ECS (Electronic Clearing Service), NEFT (National Electronic Fund Transfer), RTGS (Real-time Gross Settlement Systems), and mobile transactions is a glimpse of the deep rooted technology in banking and financial matters. With the swift expansion of computer and internet technologies, new forms of worldwide crimes known as “Cyber Crimes” have evolved in the scene. Over a period of time the Cyber Crime incidents have become more complex and modern. Banks and Financial Institutions remain the unabated targets of cyber criminals in the last decade. This paper focuses on the technical aspects of various types of cybercrimes concerning the banking and financial sector and their related impacts. Additionally, it identifies the threat vectors supporting these cybercrimes and creates measures to aid in the combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security.

Keywords: Cyber-Crime, Financial Fraud, Identity Theft

1. Introduction:

At present, the activities performed over the internet are not just limited to technology freaks for technical uses; rather every second individual is enjoying the easy internet availability and accessibility for day-to-day purposes like ecommerce, education, banking, entertainment, etc. Markedly, the wave of smart phones has definitely acted as a catalyst to this tremendous internet growth. Therefore, the web technology has emerged as an integral and indispensable part of the Indian Banking Sector. The enlargement of non-cash based transactions around the globe has resulted in the steady development of robust online payment systems. As an increasing number of users are demanding online services, the background mission of providing balanced security and convenience seems to be a tough challenge due to numerous obtrusive actors collectively referred to as “Cyber-Crime”.

Simply stated, “Cyber-Crime” is crime that involves a computer and a network. Cyber-Crime is being considered a serious threat to all the aspects of a nation’s economic growth as maximum instances of the same are being observed in financial institutions.

With the upgrade in innovation, keeping money cheats have additionally expanded. Cyber offenders are utilizing diverse intends to take one’s bank data and at last their cash also. It is in this manner, an aggregate agreement of banks and controllers to make arrangements and embrace measures so as to shield saving money stages from cyber crimes. Various specialized guard and control estimates like expanded continuous supervision on exchanges have been attempted by the banks, nonetheless, even today the issue holds on. One of the approaches to relieve the issue of cybercrimes in keeping money segment is to distinguish the variables identified with banks that are by and large focuses of such cyber-attacks, and why a few banks have never confronted such a circumstance. Banks which are for the most part focuses of cybercrimes experience the ill effects of different malware assaults in type of web based phishing, keystroke-loggings malwares, wholesale fraud, and so forth.

2. Review of Literature:

Cybercrime is the bane of the internet and new technologies generate new opportunities of more innovative ways of doing crimes and this threat is growing multi fold in this new world of digitalization and growing technology. According to a study from the University of Maryland, there is a cyber attack once every 39 seconds. This shows how the technical evolution has outpaced the defence as well as security tactics of private organisations and the government all over the world.

Claessens *et al.*, (2002) stated that there are number of cybercrimes witnessed in the banking sector, like Cyber Money Laundering, ATM frauds, and Credit Card Frauds. However, in general all the frauds are executed with the ultimate goal of gaining access to user s bank account, steal funds and transfer it to some other bank account. In some cases the cyber criminals uses the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts. Moore. T, Clayton. R and Anderson. R, (2009) focused on the subject of online crime. Online crimes mostly occur from the nuisance came from amateur hackers. They stated about the data of online crime and analysed that data. The analysis of their paper shows that significant improvements are possible in the way dealing with online fraud and to study the online crime it is suggested that to understand its economic perspective.

According to Florencio & Herley, (2011), as a lot of vulnerabilities exist in the defense system of banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and combat such crimes.

Therefore, this manuscript highlights the issue of emerging cybercrimes in banking sector with a brief overview of impact of cybercrime and safeguarding the internet banking sectors.

3. Objectives:

1. To study about cyber crime in banking sectors in detail.
2. To understand internet banking in India.
3. To study about impacts of cybercrime in the banking sectors.
4. To analyze and use the preventive measures of safeguarding the internet banking sector.

4. Cyber Crime in Banking Sector:

Cyber Crime can be simply stated as crimes that involve the use of computer and a network as a medium, instrument, target, source, or place of a crime. With the growing aspect of e-commerce and e-transactions, the economic crime has drifted towards the digital world. Cyber crimes are increasing globally and India too has been witnessing a sharp increase in cyber crimes related cases in the ongoing years. In 2016, a study by Juniper Research estimated that the global costs of cybercrime could be as high as 2.1 trillion by 2019. However such estimates are only indicative and the actual cost of cybercrime including unreported damages is beyond estimation.

Cyber Crimes can be broadly classified into categories such as Cyber Terrorism, Computer Vandalism, Online Thefts, Cyber-bullying, Software Piracy, Identity Theft, and Frauds, Email Spam, Phishing, etc. However, from the aspect of financial cyber crimes committed electronically, the following categories are predominant:

- **Hacking:** It is a technique to gain illegal access to a computer or network in order to corrupt, steal, or illegitimately view data.
- **Vishing:** It's the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward.
- **Spamming:** Unwanted and unsolicited e-mails usually sent in bulk in an attempt to force the message on people who would not otherwise choose to receive it are referred to as Spam E-mails.
- **E-mail Spoofing:** It is a technique of hiding an e-mail's actual origin by forged the e-mail header to appear to originate from one legitimate source instead of the actual originating source.
- **Phishing:** It is a technique to obtain confidential information such as usernames, passwords, and debit/credit card details, by impersonating as a trustworthy entity in an electronic communication and replay the same details for malicious reasons.
- **Advanced Persistent Threat:** It is characterized as a set of complex, hidden and ongoing computer hacking processes, often targeting a specific entity to break into a network by avoiding detection to gather sensitive information over a significant period of time. The attacker usually uses some type of social engineering, to gain access to the targeted network through legitimate means.
- **Denial of Service:** This attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service by flooding a network to disallow legitimate network traffic, disrupt connections between two machines to prohibit access to a service or prevent a particular individual from accessing a service.
- **ATM Skimming and point of sale crimes:** It is a technique of compromising the ATM machine or POS systems by installing a skimming device atop the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine. Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number (PIN) codes that are later replicated to carry out fraudulent transactions.

5. **Internet Banking in India:**

Electronic keeping money or e-managing an account alludes to a framework where saving money exercises are completed utilizing instructive and computer innovation over human asset. In contrast with customary saving money administrations, in e-managing an account there is no physical association between the bank and the clients. E-managing an account is the conveyance of bank's data and administrations by banks to clients by means of various conveyance stages that can be utilized with various terminal gadgets, for example, computer and a cell phone with program or work area programming, phone or advanced TV.

The main activity in the territory of bank computerization was stemmed out of two progressive Boards on Computerization (Rangarajan Panel). The primary board of trustees was set up in 1984 which drew the outline for the automation and computerization in managing an account industry. The second board of trustees was set up in 1989 which made ready for incorporated utilization of broadcast communications and computers for applying completely the innovative leaps forward to the managing an account tasks. The center moved from the utilization of cutting edge Record Posting Machines (ALPMs) for constrained computerization to full computerization at branches and to combination of the branches. Till 1989, banks in India had 4776 ALPMs at the branch level, more than 2000 software engineers/frameworks staff and more than 12000 Information Passage Terminal Administrators.

The RBI (Reserve Bank of India) established a working gathering on web managing an account. In light of the idea of access to the managing an account items and administrations, the gathering partitioned web keeping money into three frameworks.

- **Enlightening Framework:** This framework expects banks to give data about financing costs, branch areas, and credit plans to the clients. The client can download different kinds of utilization according to the necessities. Additionally clients are not required to uncover their personality and there is no sensible possibility of any unapproved individual getting into the creation arrangement of the bank.
- **Open Framework:** This framework gives data to the client about his exchange subtleties, record balance, and so on. The clients can look for the data after confirmation and signing in through the passwords.
- **Value-based Framework:** In this framework a bank enables its clients to embrace exchanges through its framework and they are straight forwardly transferred to the client's record. There is bi-directional exchange that happens between the bank and the client and between the client and the outsider. This framework is anchored through security instruments like http and https. E-keeping money is otherwise called Digital Saving money, Home Saving money and Virtual Saving money, E-keeping money incorporates Web Saving money, Portable Managing an account, RTGS, ATMs, MasterCard's, Charge Cards, and Keen Cards and so forth.

6. Impacts of Cyber Crime in the Banking Sector:

The cases related to cybercrimes have grown ruthlessly due to the upsurge in mobile devices with internet connectivity. Smart phones are nowadays used for numerous online activities like online shopping, internet banking, paying utility bills and are constantly in the eyes of the criminals to obtain access to confidential information.

Amongst the various motivations for committing a cybercrime, Financial Gain remains the constant winner for the past many years overtaking other motives including revenge, extortion and political causes. (Fig 1)

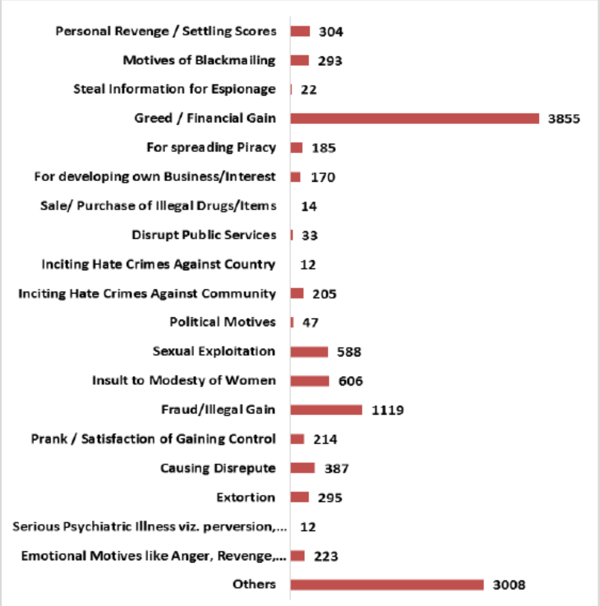

Fig 1: Cyber Crime by Motives

Alarmingly, simple phishing attacks enjoy a success rate of 45% due to lack of awareness regarding the common safeguards to protect against the shrewd cyber criminals.

The span of cybercrime can be estimated from the figures of 3855 cybercrimes committed for financial gain (NTRO) and 534 phishing incidents (CERT-In) in year 2015. These incidents only correspond to the reported incidents and do not comprise the incidents that went unreported and/or unnoticed.

Banks across the globe are increasing becoming prime targets of distributed denial-of-service (DDoS) attacks launched sometimes as a part of the plan to distract the security professional’s attention to the depleting resources, while carrying out some additional dangerous activity in parallel like insertion of malware, or tampering with the IT assets. Such an embedded hacking campaign with a hidden agenda is usually referred to as Advanced Persistent Threat and is the latest kid on the board with enhanced complexity and shrewdness.

In the cases, where the attackers are not able to yield some valuable information, they deface the banks website as a measure to take revenge against their failed attempts.

Besides the resulting financial gains from successful cyber attacks, the presence of online black markets commonly referred to as the “Darkweb” ads to the motivation of committing cybercrimes as a common place for exchanging personal information, latest exploits and sophisticated hacking kits. Sensitive information including stolen/leaked credit card numbers, online banking accounts, medical records and administrative access to servers are traded for money in these online fraud communities.

7. Safeguarding the Internet Banking Sector:

Financial organizations in today’s date require well laid cyber security teams with distinguished digital leaders. According to PWC’s year’s global economic crime survey, 2016, too many organisations are leaving first response to their IT teams without adequate intervention or support from senior management and other key players. Specialized security teams with an upbeat mix of competent professionals should be employed to take a proactive stance when it comes to cyber security and privacy.

Organizations in the BFSI sector need to undergo rigorous and continuous cybercrime risk assessments to precisely assess identify and improve their present security posture by viewing the organization's policies from an attacker's perspective and thus facilitate enhanced security, operations, organizational management. Additionally, as long-term planning, cyber awareness needs to introduced at a fundamental level in educational institutions and graduate level to provide hands-on training on the latest attack and mitigation techniques.

A comprehensive threat intelligence technology is essential to foster organized and analysed threat information about potential or current attacks from the organization's perspective. Alongside, threat intelligence helps organizations in understanding the common threat actors including latest vulnerabilities, exploits and advanced persistent threats (APTs) campaigns.

On a national level, there is an urgent necessity of building capability of inspecting critical infrastructure in critical industry sectors before these are deployed in production to avoid any malicious intruders by leveraging the trusted hardware/software. Finally cooperation amongst Indian government sector and industrial groups is bound to strengthen the legal framework for cyber security with each blending in a different array of cyber risks and preventive mechanisms.

8. Conclusion:

There is a need to forestall cybercrime by guaranteeing validation, recognizable proof and check procedures when an individual goes into any sort of saving money exchange in electronic medium. The development in cybercrime and intricacy of its examination strategy requires proper measures to be embraced. It is basic to expand the collaboration between the partners to handle cybercrime.

In instances of cybercrime, there isn't just money related misfortune to the banks yet the confidence of the client upon banks is additionally undermined. Indian managing an account division can't abstain from keeping money exercises helped out through electronic medium as the investigation recommend that there has been an expansion in the quantity of installments in e-saving money. Nonetheless, the adjustment in the saving money industry must be such which suits the Indian market.

It may also be presumed that to dispense with and kill cybercrime from the internet is certifiably not an apparently conceivable assignment however it is conceivable to have an ordinary keep an eye on managing an account exercises and exchanges. The main auspicious advance is to make mindfulness among individuals about their rights and obligations and to additionally making the usage of the laws all the more firm and stringent to check cybercrime.

References:

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Hussain, W. S., & Ibrahim, N. J. (2019). A Survey of Cybercrimes, Investigations and Penal Laws Imposed on the Criminals.

Kruse, I. I. (2002). WG and Heiser, JG Computer forensics: incident response essentials.

Moore, R. (2005). Cybercrime: Investigating high-technology computer crime. LexisNexis.

Morgan, S. (2016). Cyber crime costs projected to reach $2 trillion by 2019. *Forbes. Retrieved September*, *22*(2016.1).

Murashbekov, O. B. (2015). Methods for Cybercrime Fighting Improvement in Developed Countries. *The Journal of Internet Banking and Commerce*.

Murphy, E. M. Judgments entered against defendants for distributing unregistered shares of universal express inc.

Rao, H. S. (2019). Cyber crime in banking sector. *International Journal of Research-GRANTHAALAYAH*, *7*(1), 148-161.

Sandle, P., & Char, P. (2014). Cyber crime costs global economy $445 billion a year: report. *Reuters.*

*****