

CYBER-CRIME: A GROWING THREAT TO INDIAN BANKING SECTOR

Seema Goel

New Delhi, India

ABSTRACT

The banking industry has enjoyed the ride of emerging technology to undergo significant changes. Banks are among the biggest beneficiaries of the IT revolution and have largely adopted Information Technology solutions for rendering the banking services to their customers. The proliferation in online transactions mounting on technologies like NEFT (National Electronic Fund Transfer), RTGS (Real-time Gross Settlement Systems), ECS (Electronic Clearing Service) 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” has evolved in the scene. Over a period of time, the nature and pattern of Cyber Crime incidents have become more sophisticated and complex. Banks and Financial Institutions remain the unabated targets of cyber criminals in the last decade. Notably financial gain is still one of the major motivations behind most cybercriminal activities and there is little chance of this changing in the near future (Symantec, 2015).

This paper focusses 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 develop 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

I. INTRODUCTION

The world is fast moving online with 46.1% of total world population now connected to the web according to internetlivestats.com (as on July 1, 2016). A remarkable instance of this phenomena has been experienced in India with a notable increase in the past three years i.e. 18% of the Indian population online in 2014, 27% in 2015 and 34.8% in 2016 (as on July 1, 2016).

Today 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 banking, ecommerce, education, entertainment and many more. Markedly, the wave of smartphones has definitely acted as a catalyst to this tremendous internet growth.

As an increasing number of users are demanding online services, the background mission of providing balanced security and convenience is seeming 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. (Moore R, 2005).

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.

Cyber-Crime incidents include but are not limited to credit card fraud, spamming, spoofing, e-money laundering, ATM fraud, phishing, vishing, identity theft and denial of service.

II. PROBLEM STATEMENT

Today, 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.

While paper-based transactions cleared through cheques amounted to Rs 85 lakh crore in FY15, paperless transactions, including retail electronic transactions such as ECS (electronic clearing system) debits and credits, electronic fund transfer, card transactions, mobile transactions and prepaid instruments were to the tune of Rs 92 lakh crore in the same.

India has seen an upsurge in the volume of debit/credit cards due to increased online acceptance through alternative channels, including internet, ATM and mobile banking. In the days to come, this volume will gain traction as the youth generation will enter the economic gyration.

The last few years have seen a significant increase in cybercrime across all sectors and geographies. Given the proliferation of these technological crime, organisations face a significant challenge to be resistant against cyberattacks. As per Motive-wise Cases Reported under Cyber Crimes during 2015 statistics by National Crime Records Bureau, Greed / Financial Gain is the prime motivation for committing Cyber Crimes.

This research attempts to analyse the concerns of cyber threats to the banking sector by highlighting the underlying modus operandi. It focusses on the preparedness of the financial organisations to deal with incidents related to Cyber Crime.

III. CYBER CRIME IN BANKING SECTOR

Cyber Crime can be simply stated as crimes that involve the use of computer and a network^[2] as a medium, source, instrument, target, 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 recent 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.^[1] 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, Cyber-bullying, Computer Vandalism, Software Piracy, Identity Theft, Online Thefts and Frauds, Email Spam and Phishing and many more.

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 steal, corrupt, or illegitimately view data.
- **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.
- **Vishing:** It is 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.^[3]
- **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.
- **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.
- **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.^[4]
- **Advanced Persistent Threat:** It is characterised 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.
- **Advanced Persistent Threat:**
It is characterised 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. Successful advanced persistent threat campaigns can result in costly data breaches.
- **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

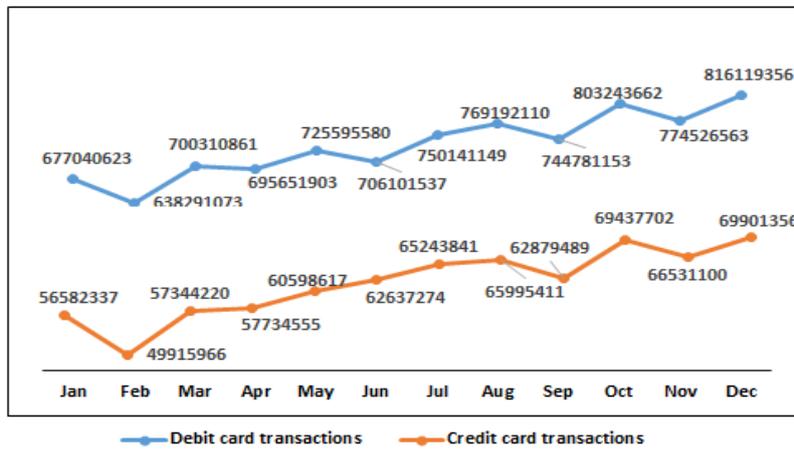
implementation of skimmers cause in ATM machine to collect card numbers and personal identification number (PIN) codes that are later replicated to carry out fraudulent transactions.

IV.OVERVIEW OF INTERNET BANKING IN INDIA

The Indian banking industry is enjoying a joyous growth. With the credit card and debit card users increasing everyday and new technologies like internet wallets slowly gaining popularity, the financial transactions are touching all-time highs.

This firm progression in the mounting paper less transactions numbers where a total of 9545797438 transactions were commenced using credit and debit cards in the year 2015 alone (Fig 1) can be partially accredited to the recent developments in the e-banking and e-commerce verticals.

Fig 1: Credit/Debit Card Transactions in



In order to provide improved support for cashless transactions, a steady increase in the number ATM and POS machines is inevitable. Fig 2 highlights the growth in the number of ATM machines and POS machines installed across India in 2015.

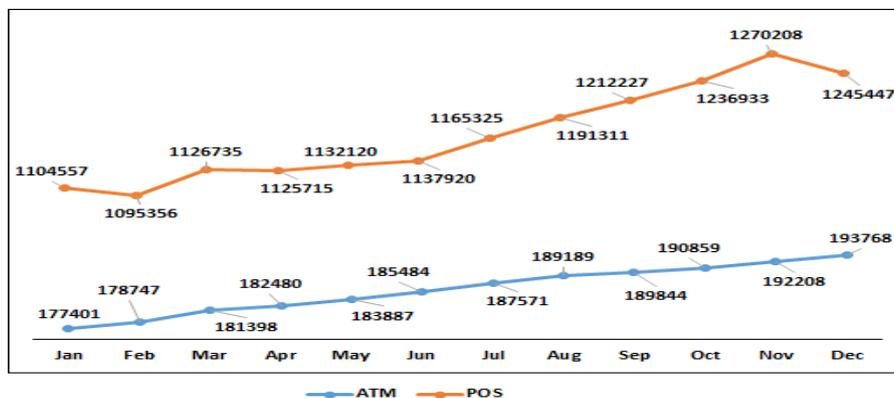


Fig 2: ATM & POS Transactions in

V.IMPACTS OF CYBER CRIME ON THE BANKING SECTOR

The cases related to cybercrimes have grown ruthlessly due to the upsurge in mobile devices with internet connectivity. Smartphones are nowadays used for numerous online activities like internet banking, online shopping, 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 3)

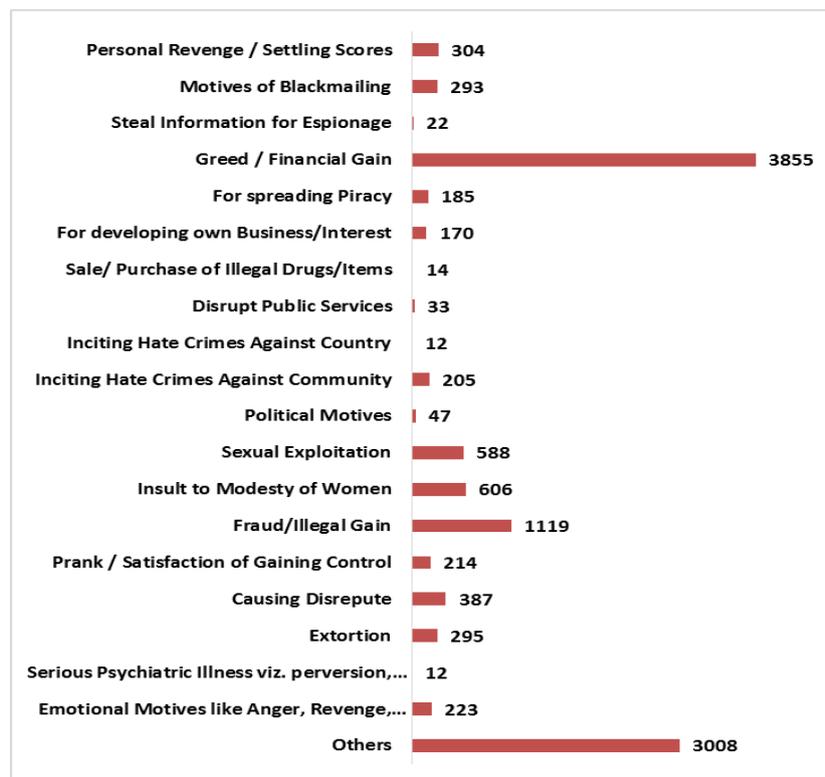


Fig 3: Cyber Crime by Motives

Alarming, 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'^[5] adds to the motivation of committing cybercrimes as a commonplace 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.

VI. CONCLUSION

Indian customers are gradually preferring online services because of convenience, cost-saving and swiftness of online transactions. In addition, financial institutions are tossing exciting offers to customers with the vision of upturning the volume of cashless transactions due to comparatively lower operational costs.

However, it can be concluded the cyber security measures placed by financial institutions to curtail the curse of cybercrime are being out- paced by dynamic technological landscape and improved expertise of the intruders.

Amidst the continuous upliftment of the technology implemented at the backend of the financial institution, some essential aspects were overlooked that now demand huge attention.

Cybercrime comprises its own set of unique attractive features that have gradually started outweighing the traditional crimes. The extent of anonymity, global victim reach and swift results are amongst the few that cybercriminals find most attractive.

Non-existent/Inadequate awareness campaigns further simplifies the work of the cyber criminals. Unaware consumers are easily deceived due to lack of insight into the latest attack methodologies and identified preventive measures.

Additionally, traditional law enforcement policies, standards and methods have been proved insufficient to cater to the evolving cybercrimes and the IT Act of India has been marked down time and again. On 13 April 2015, it was announced that the Ministry of Home Affairs would form a committee of officials from the Intelligence Bureau, Central Bureau of Investigation, National Investigation Agency, Delhi Police and ministry itself to produce a new legal framework.^[6]

With the increasingly notable impact of the peril of cybercrime, it has been continuously realised that local law enforcement agencies do not have the required skills and resources to investigate incidents related to cybercrimes. Engagement of specialized cyber security professionals is a step further to derive quicker and better

cybercrime investigation results. As estimated by NASSCOM's Cybersecurity Task Force, India needs 1 million trained cyber security professionals by 2025.

VII. 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 cybersecurity 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 need to be introduced at a fundamental level in educational institutions with specialized security courses at graduate level to provide hands-on training on the latest attack methodologies and mitigation techniques using concepts like virtual cyber labs.

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 cybersecurity with each blending in a different array of cyber risks and preventive mechanisms.

REFERENCES

- [1] Liu, J., Heberton, B., & Jou, S. (n.d.). Handbook of Asian Criminology.
- [2] Kharouni, L. (2012). Automating Online Banking Fraud Automatic Transfer System: The Latest Cybercrime Toolkit Feature (Rep.).
- [3] Threats to the Financial Services sector (Rep.). (2014). PricewaterhouseCoopers.
- [4] Net Losses: Estimating the Global Cost of Cybercrime (Rep.). (2014). Intel Security.
- [5] Murashbekov, O B. (2015). Methods for Cybercrime Fighting Improvement in Developed Countries. Journal of Internet Banking and Commerce.

3rd International Conference on Recent Innovations in Science, Technology, Management and Environment

Indian Federation of United Nations Associations, New Delhi, India

(ICRISTME-16)

18th December 2016 , www.conferenceworld.in

ISBN: 978-93-86171-13-9

[6] Fianyi, I. D. (2015, November 06). Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics. International Journal of Computer Science Issues.

[7] The Economic Impact of Cybercrime and Cyber Espionage (Rep.). (2013). McAfee.