International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

CYBER-CRIMES: A Growing Threat to Indian Banking Sector

Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru
Students
St. Joseph's Degree & PG College

Mrs. Shanit Kiran
Assistant Professor
St. Joseph's Degree & PG College

ABSTRACT: *With the advancements in technology, the Indian Banking Sector has been at par with the emerging trends and significant changes required in its operations. The call for growth has given this unit immense opportunities and as a result, banks are now among the biggest beneficiaries of the IT Revolution. The proliferation in online transactions mounting on technologies like NEFT (National Electronic Fund Transfer) , RTGS (Real-Time Gross Settlement) , ECS (Electronic Clearing Service) and mobile transactions is a glimpse of the deep rooted technology in banking and financial matters. But like two sides to a coin, opportunities come with threats and success comes with its equivalent challenges. Thus, with the swift expansion of computers and internet technology, 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 the major motivation behind most cybercriminal activities and there is little chance of this changing in the near future. This paper focuses on the technical aspects of various types of cybercrimes concerning the banking units and their related impacts. Additionally, it identifies the threat vectors supporting these crimes and develops measures to aid in combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security.*

Keywords: Cyber-Crime, Financial Fraud, Fraud Detection, Identity Theft

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

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

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 amounting 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. The last few years have seen a significant increase in cybercrime across all sectors and geographies. Given the proliferation of these technological crimes, organizations face a significant challenge to be resistant against cyber-attacks. 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 analyze the concerns of cyber threats to the banking sector by highlighting the underlying modus operandi. It focuses on the preparedness of the financial organizations to deal with incidentsrelated to Cyber Crime.

NEED FOR STUDY

There is a need to identifystudy and analyze the loopholes existing in the Indian Banking Sector in order to curb the fraudulent activities and to be able to take corrective actions, therebyenhancing the security measures of this sector.

OBJECTIVES OF THE STUDY

1. To understand how cybercrime operations work and why they make money
2. To study cybercrimes and itsimplications on the Banking Sector
3. To understand fraud\ fraud detection in the sector under study
4. To identify the complaints received, solved and pending
5. To analyze and use the preventive measures available to control frauds

LIMITATIONS

The scope of the study is limited to the banking sector only, all aspects, points and measures covered under the study are relevant and restricted to the banking sector and does not exceed beyond that**.**

RESEARCH METHODOLOGY

The data used is completely secondary in nature i.e., from sources published, printedmedia, magazines and journals

HOW CYBERCRIME OPERATIONS WORK – AND WHY THEY MAKE MONEY

The rise of cybercrime is inextricably linked to the ubiquity of credit card transactions andonline bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency.The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations ofrisk, expense and skill. The most straightforward is to buy the ‘finished product’. In this case we’ll use the example of an online bank account. The product takes the form of information necessary to gain authorized control over a bank account with a six-figure balance. The cost to obtain this

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

information is $400 (cybercriminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it's very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia. The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chatroom. The $400 fee will most likely be exchanged in some form of virtual currency such as e-gold.Not all cyber-criminals operate at the coalface, and certainly don't work exclusively of one another; different protagonists in the crime community perform a range of important, specialized functions. These broadly encompass: Coders – comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, 'coders' produce ready-to- use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cybercrime labor force – the 'kids'. Coders can make a few hundred dollars for every criminal activity they engage in. Drops – the individuals who convert the 'virtual money' obtained in cybercrime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent 'safe' addresses for goods purchased with stolen financial details to be sent, or else 'safe' legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately. Mobs – professionally operating criminal organizations' combining or utilizing all of the functions covered by the above.

So why are banks such a lucrative target for cybercrime? The answer is simple, cyber criminals go where the money is, and banks have more money than most other organizations.While there are numerous threats aimed at bank systems and their customers, one of the biggest threats, and often one of the hardest to detect, is that of malicious, careless and compromised users. These employees, contractors and partners are already inside the banks secure perimeter and have legitimate access to its sensitive data and IT systems. Besides, gaining control of a bank account is increasingly accomplished through phishing. There are other cybercrime techniques, but space does not allow their full explanation.

CYBER CRIMES IN THE BANKING SECTOR

Cyber Crime can be simply stated as crimes that involve the use of computer and a network 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. Cybercrimes are increasing globally and India too has been witnessing a sharp increase in cybercrime related cases in the recent years. As financial institutions shift to digital channels like online banking and mobile transactions, the attack surface grows, and there is more to protect. Combine this with the fact that successful attacks on banks and financial services firms provide a quick way to monetize the data, and you can see why banks and financial institutions are such popular targets.

FRAUD/FRAUD DETECTION

Nowadays, the banking industry is facing an acute problem of fraud. The problem is global, and no country is fully protected. Fraudsters have become experts in hijacking online sessions: they steal client credentials and use malware to swindle funds from unaware account holders. In his book "Future Crimes" Marc Goodman explains that "criminals are often the first to exploit emergent technologies and turn their complexity against their users". One of these options is the use of data analysis software which, in most cases, guarantees impeccable fraud detection. Modern systems allow fraud examiners to analyze business data and check how well the internal control system is operating.

As the result, they can designate transactions that denote fraudulent activity or the elevated risk of fraud. There is a spectrum of analysis measures that can be applied to tackle fraud. It ranges from contextual situations for a singular fraud investigation to a repeatable analysis of financial processes susceptible to criminal activity in the first place. If the risk of fraud is really high, financial and banking institutions can

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

employ a constant or continual approach to fraud detection. It works particularly well in situations where preventive controls are not practicable or efficient. The majority of modern financial service companies have increased management requirements for information as the audit adjustment is moving from the conventional cyclical approach to a risk-based and longstanding model. To disclose fraudulent activity, a lot of banks use special transaction monitoring systems. By and large, they represent domestically produced software which demands an operator intervention. However, traditional security systems can function well for detecting individual point-of-sale, real-time fraud. But that is only the tip of an iceberg.

There is a list of analytical techniques used to detect fraud. The most effective among them are –

1) Classification: - to find patterns among various data elements

2) Statistical parameters calculation (standard deviation, averages, etc.): - to detect outliers that could reveal fraud.

3) Numbers stratification: - to disclose unordinary (redundantly high or low) entries.

4) Joining random diverse sources: - to denote matching values (such as names addresses and account numbers) where they shouldn't exist.

5) Duplicate testing: - to note duplicate transactions such as claims, payments or financial report items

6) Gap testing: - to find out any missing items in a serial data where there should be none

7) Entry dates validation: - to estimate inappropriate or suspicious items or postings or information entry

8) Numeric values summation: - to identify control sums which may have been falsified

THE COMPLAINTS RECEIVED, SOLVED AND PENDING

As per the data made available by the Reserve Bank of India, 13,083 and 11,997 cases related to ATM/credit/debit cards and net banking frauds were reported by the banks during 2014-15 and 2015-16 (up to December 2015), respectively.

Besides, 44,679 and 49,455 cyber security incidents including phishing, scanning, malicious code, website intrusion, denial of service etc. were reported during the year 2014 and 2015, respectively, as per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In). The above cases were registered with banks. The following cases were registered with cyber-crime department of police the cases of banking frauds — phishing, cyber stalking, impersonation on social media sites, and job and lottery frauds registered with the city's cyber police department in the year 2016 have decreased significantly. However, the number of cases solved by the cyber cell has remained consistently low for the last four years, with only 20 per cent success rate. Eighty per cent of the crimes registered in the year 2016 remain undetected, according to the report shared by the cyber cell. It also reveals that the total number of cases registered in the year 2016 has gone down by 50 per cent Vis-a- Vis the last year. Two eighty two cases were registered in 2015, which dipped to 145 in 2016

PREVENTIVE MEASURES TO CONTROL FRAUDS

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 organizations 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

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

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, organizationalmanagement.Additionally, as long-term planning, cyber awareness need to introduced at a fundamental level ineducationalinstitutions 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 analyzed 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.

AI TECHNOLOGY AND FRAUD PREVENTION

It's fair to say that AI has become quite a buzzword in various fields of business. The financial services industry is no exception. Originally introduced in the 1950s, AI has gained a new wave of popularity just recently due to the variety of reasons. One of them is, obviously, the adoption of new standards in security. The industry in whole moves to embrace promising technologies, and many bank institutions are already heading in that direction. As Narrative Science report says, 32% of respondents among banks confirmed using AI technologies such as predictive analytics, recommendation engines, voice recognition and response. Again, one of the most important uses of artificial intelligence in banking sphere concerns fraud detection. Banks are beginning to utilize AI to fight against cybercrime and address complex issues in real time. Over the last ten years, AI has significantly improved the monitoring process: now it's is capable of learning in a fast-paced environment and respond to fraudsters' techniques as they appear. Let's take bank accounts. When an account activity is being monitored, some user patterns can be distinguished. This way, if there's a sign of any abnormal activity, it's being flagged for review. So, when a customer is trying to make a purchase using a debit or credit card, the detection mechanism can analyze transactions within 0.3 seconds, detecting fraud or approving non-fraudulent transactions without interruption to purchases. Such systems are trained to recognize potential fraud through supervised training, when the variety of random samples is manually classified as genuine or fraudulent. Subsequently, the algorithm learns from these manual classifications to determine the legitimacy of future activities on its own. Within several years, the strategic use of AI and machine learning will become an integral part of banking organizations' security principles. AI can save banks considerable money by eliminating complex fraud cases and protecting their brand. Within several years, the strategic use of AI and machine learning will become an integral part of banking organizations' security principles. AI can save banks considerable money by eliminating complex fraud cases and protecting their brand.

CASE UNDER THE STUDY: (EXAMPLES)

OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKEDMUMBAI,

20 September 2007 — IT experts were trying yesterday to restore the official website of the government of Maharashtra, which was hacked in the early hours of Tuesday. Rakesh Maria, joint commissioner of police, said that the state's IT officials lodged a formal complaint with the Cyber Crime Branch police on Tuesday. He added that the hackers would be tracked down. Yesterday the website, http://www.maharashtragovernment.in, remained blocked. Deputy Chief Minister and Home Minister R.R.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

Patil confirmed that the Maharashtra government website had been hacked. He added that the state government would seek the help of IT and the Cyber Crime Branch to investigate the hacking. “We have taken a serious view of this hacking, and if need be the government would even go further and seek the help of private IT experts. Discussions are in progress between the officials of the IT Department and experts,” Patil added.

The state government website contains detailed information about government departments, circulars, reports, and several other topics. IT experts working on restoring the website told Arab News that they fear that the hackers may have destroyed all of the website’s contents. According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as “Hackers Cool Al-Jazeera” and claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail. According to a senior official from the state government’s IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall. Three people held guilty in on line credit card scam Customers credit card details were misused through online means for booking air-tickets. These culprits were caught by the city Cyber Crime Investigation Cell in Pune. It is found that details misused were belonging to 100 people. Mr. Parvesh Chauhan, ICICI Prudential Life Insurance officer had complained on behalf of one of his customer. In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested. Lukkad being employed at a private institution, Kale was his friend. Shaiklh was employed in one of the branches of State Bank of India. According to the information provided by the police, one of the customers received a SMSbased alert for purchasing of the ticket even when the credit card was being held by him.Customer was alert and came to know something was fishy; he enquired and came to knowabout themisuse. He contacted the Bank in this regard. Police observed involvement of many

Banks in this reference -The tickets were book through online means. Police requested for the log details and got the information of the Private Institution. Investigation revealed that the details were obtained from State Bank of India. Shaikh was working in the credit card department; due to this he had access to credit card details of some customers. He gave that information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale Lukkad booked tickets. He used to sell these tickets to customers and get money for the same. He had given few tickets to various other institutions. Cyber Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate were involved in eight days of investigation and finally caught the culprits. In this regards various Banks have been contacted; also, four air-line industries were contacted. DCP Sunil Pulhari has requested customers who have fallen in to this trap to inform police authorities on 2612-4452 or 2612-3346 if they have any problems.

UTI Bank hooked in a phishing attack(14 February 2007)

Fraudsters of cyberspace have reared its ugly head, the first of its kind in the year 2007, by launching a phishing attack on the website of Ahmedabad-based UTI Bank, a leading private bank promoted by India’s largest financial institution, Unit Trust of India (UTI).A URL on GeoCities that is almost a facsimile version of the UTI Bank; s home page is reported to be circulating amongst email users. The web page not only asks for the account holder’s information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements. In case you have received any e-mail from an address appearing to be sent by UTIBANK, advising you of any changes made in your personal information, account details orinformation on your user id and password of your net banking facility, please do not respond. It is UTI Bankpolicy not to seek or send such information through email. If you have already disclosed your password please change it immediately, the warning says. The tricky link is available on http://br.geocities/ If any unsuspecting account holder enters his login id, password, transaction id and password in order to change

his details as advised by the bank, the same info is sent vide mailform.cz (the phishes database). After investigation, we found that Mail form is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named PetrStastnywhose e-mail can be found on the web page. Top officials at UTI Bank said that they have reported the case to the Economic Office Wing, Delhi Police. The bank has also engaged the services of Melbourne-based Fraud Watch International, a leading anti-phishing company that offers phishing monitoring and take-down solutions. We are now in the process of closing the site. Some of these initiatives take time, but customers have been kept in the loop about these initiatives, said V K Ramani,

President - IT, UTI Bank

As per the findings of UTI Bank's security department, the phishers have sent more than 1,00,000 emails to account holders of UTI Bank as well as other banks. Though the company has kicked off damage control initiatives, none of the initiatives are cent percent fool proof.

Now there is no way for banks to know if the person logging-in with accurate user information is a fraud, said Ramani. However, reliable sources within the bank and security agencies confirmed that the losses due to this particular attack were zilch. The bank has sent alerts to all its customers informing about such malicious websites, besides beefing up their alert and fraud response system; Engaging professional companies like Fraud Watch help in reducing time to respond to attacks; said Sanjay Haswar, Assistant Vice President, Network and Security, UTI Bank.

FINDINGS OF THE STUDY

- Majority of the cybercrimes in this sector have resulted out of hacking and identity theft.
- Banks are being targeted over and over again because all the reserves in the form of cash are held with the banks.
- The security of the customers is at a huge risk since it has become very easy to hack their personal details.
- The software used for detecting frauds in most cases is either outdated or very time consuming.
- The number of cases solved by the cyber cell has remained consistently low for the last four years, with only 20 per cent success rate.
- There is no specific enactment that deals with these crimes, in particular with the Banking Sectors.

SUGGESTIONS

- As there is no specific enforcement related to the law, the major impact of these crimes is left unsolved many a times, an act has to be enforced to curb this kind of menace.
- The law enforcement should be very rigid, and updated from time to time to keep a track of such crimes.
- There should be fast track mobile courts to solve these cases, to meet the grievances and build confidence among the public.
- The government should also keep a track on the operating network activities with the help of Big Data Banks.
- Punishments and penalties need to be exercised thoroughly in order to minimize the impact of these issues and penalize the attackers.
- Awareness Programmes should be initiated in order to inform the public about the ongoing scenario and upcoming threats.
- The public should report these cases to the Cyber Crime Branch in the matters related rather than just referring it to the banks, so as to ensure fast and strict actions.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

CONCLUSION

In the selected subject of work, we made a thorough study on the new forms of crimes. The criminals of this advanced age endeavor to commit these new crimes with the help of computers through Internet by exploiting cyber space. An estimated 95% of transactions in India are paid for in cash but with the growing penetration of computers and smartphones, and increasing access to the internet, Indians are taking to digital channels for their banking needs. Cybercrime is becoming a greater threat as a result.

The RBI classifies bank fraud as transactions involving any cheating, negligence, misappropriation of funds, or forged documents. “Not only simple attacks using phishing, vishing and social engineering, but also increasingly audacious attacks by organized gangs with or without backing by state players have come to light,” the RBI said. The RBI recommended that banks invest in preventive software and frequently assess the risks at hand, not just for in-house operations but also for the external vendors that the lenders employ. This can be understood as a great plan if implemented rightly, since hackers always invade into the private details of the customer’s and\or of banks, as the case maybe. They tend to formulate innovative ways to commit these crimes and before one can figure out what went wrong, the damage has already been caused, that is the intensity and speed of such fraudulent transactions which take place in fraction of seconds. The time has come to consider the impact of such type of crimes on the society with due perspective, so that the cyber criminals don’t go escort free. The cybercrime is a primarily example of cross-border crime. Since the jurisdiction in this area is a tricky and is still unclear, it is important that we recognize the need of the hour and stand for a serious cause, against cybercrimes and more so pertaining to the banking sector as the financial security of this sector defines the financial security and safety of the assets of our nation as a whole. India, being at its stage of development, we cannot risk the safety of such an essential unit. If we are able to curb these attacks, one by one, soon in the time to come, this move will help us accelerate the rate of overall growth and development and take further steps towards betterment.

REFERENCES

1. http://www.cyberlawsindia.net/
2. https://m.rediff.com/amp/business/report/perfin-if-you-are-a-victim-of-banking-fraud-heres-what-you-can-do/20150720.htm
3.https://www.google.co.in/url?sa=t&source=web&rct=j&url=http://m.timesofindia.com/business/india-business/demonetisation-case-ed-files-first-chargesheet-involving-axis-bank-staff/amp_articleshow/56959891.cms&ved=0ahUKEwi4q-6ykcHYAhVEpI8KHRX9ANoQFggtMAI&usg=AOvVaw0raptkss_InrNtSSoNpTM2&ampcf=1
4.https://www.google.co.in/url?sa=t&source=web&rct=j&url=https://m.economictimes.com/industry/banking/finance/banking/hdfc-bank-begins-probe-after-staff-held-in-money-laundering-case/amp_articleshow/49365032.cms&ved=0ahUKEwilwZuOkcHYAhVLP48KHT4rC0kQFggnMAE&usg=AOvVaw3RKUP0SVWnDDJWUy3OvmSZ&ampcf=1
5. www.conferenceworld.in
6. www.thehindubusinessline.com
7. https://www.journalguide.com/journals/international-journal-of-cyber-criminology
9.http://www.sciencedirect.com/science/article/pii/S1742287605000915
8. Wikipedia