Abstract - The human society has undergone big changes from time to time with rapid pace at social level from the beginning and technological level ever since the rise of technologies. This technology word changes the human life in every manner and every sector. Banking field is one of them. Most of the customers use electronic banking for their routine transactions and practice the various electronic services provided by banks. The banking sector applying different ways to provide facilities and securities to a man regarding to money. Security issues play extremely important role in the implementation of technologies especially in banking sector. Further on it becomes more critical when it comes to the cyber security which is at the core of banking sector. After the arrival of Internet, this banking sector is totally change specially in terms of security because now money is in your hand on a single click. Now user has number of choices to manage his money with different kind of methods. There exist some risks and some ways that we can deal with those risks that we are going to emphasize in this paper.

Keywords: Cybercriminals; Financial System; Cyber security;

I. INTRODUCTION

Crime is a social and economic phenomenon and is old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment”. The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin “the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences”. Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. The Information Communication Technology (ICT) has revolutionized different aspects of human life and has made our lives simpler. It has been applied in different industries and has made business processes simpler by sorting, summarizing, coding, and customizing the processes.

However, ICT has brought unintended consequences in form of different cybercrimes. Cybercrimes have affected different industries and banking sector is one of them which has witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, Denial of Service. The financial loss in the banking sector is huge across the globe both in terms of combating the cyber-attacks and on development of systems, so that such attacks need to be prevented in the future.

Until mid ’90s, banking sector in most parts of the world was simple and reliable; with the arrival of technology, the banking sector suffered a huge (Jaleshgari, 1999). Banks in order to enhance their customer base introduced many platforms through which transactions could be done without much effort (Vrancianu and Popa, 2010). These technologies enabled the customer to access their bank finances 24*7 and year around through, ATMs and Online banking procedures. However, with the enhancement in technology, banking frauds have also increased. Cybercriminals are using different means to steal ones bank information and ultimately their money as well (Choo, 2011). The results of study conducted revealed that globally, the banks have incurred billions of dollars in losses; and provides details of cybercrimes conducted across the globe in banking sector.

For this reason exist a consensus of banks and regulators to make policies and adopt measures in order to protect banking platforms from cyber crime (Anderson et al, 2012). A number of technical defense and control measures like increased real time supervision on transactions are made by the banks, however, even today the problem is present. The reason behind this is that the defense measures currently available with banks are often reactive, time consuming and available in public domain which can be accessed even by the cybercriminal who in turn adopts measures to combat from these defenses. The attackers allocate their time in developing new means for cybercrime and also simultaneously work on finding the solutions to bridge these defense measures. One of the ways to decrease the the problem of cybercrimes in banking sector is to identify the factors related to banks that are targets of such cyber-attacks,
and why some banks have never encountered such a situation. According to a study, some banks are targeted more frequently than others, generally by a financial malware. Banks which are targets of cybercrimes suffer from various malware attacks in form of online phishing, keystrokeloggings malwares, identity theft, etc. Some of main factors which were identified in the study which reflects the pattern why some banks are targeted more than other include their size, their authentication system is weak, the number of clients, their money transfer policies are not safe and the country in which these banks are located is also an important pre-requisite for the cyber criminals. Studies conducted recently concluded that some of the malware used to attack these banks are becoming more specific (TrendMicro, 2013).

II. PROBLEM STATEMENT

Cybercrime is a growing threat in the virtual world because individuals and organizations are relying more on internet. The use of internet and other technologies have enhanced the risk of attack from cyber criminals across the globe. With problems like; phishing, computer viruses, hacking, on the rise, we need to explore for cybercrime.

What we know is that last year technology is become important for banking sector and this offer opportunities for increase the number of customers but we should not ignored that some of customers often feel reluctant and insecure in opting for such services. There is a need for the banks to evaluate their current operating practices.

III. CYBERCRIME IN BANKING SYSTEM

In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to different account are tagged as banking frauds (Wall, 2001).

There are number of frauds or cybercrimes in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the frauds are executed with the final 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. As we know that exist some issues 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 are realized in this area which would suggest ways to mitigate the risks and combat such crimes (Florêncio & Herley, 2011; McCullagh & Caelli, 2005).

To understand more the fraud system in banking sector we will have to understand and describe the attackers and defenders in this system. The following section describes the different actors which are involved in cybercrimes.

IV. ACTORS OF BANKING FRAUD

The banking fraud can be categorized into four actor categories; malicious exploiters, money mules, victims, and security guardians.

- **Cyber Criminals**

These malicious exploiters can be categorized into five sub categories. Innovators (who seek to find security holes in the system to overcome protection measures adopted by the banks). Amateur (who are beginners in this area and their expertise is limited to computer skills, which is exploited by the cyber criminal). Insiders (who are working within the bank to leak out important information in order to take some kind of revenge). Copy cats (they are interested in recreating simple tasks). Criminals (highly organized and very knowledgeable who may use all the above mentioned actors for their own profit).

- **Money Mules**

As per the definition given by OECD report (2007), money mules are individuals recruited wittingly and often unwittingly by criminals, to facilitate illegal funds transfers from bank accounts. According to the FBI (Federal Bureau of Investigation), these individuals engage in the money transfer activity in exchange of some percentage of that money. According to Florêncio and Herley (2010) there role is to convert reversible traceable transactions into irreversible untraceable ones.

- **Victims**

Victims, according to OECD (2007), in the banking sector can be categorized into two categories; banks and users of these banks. The users or customers can be individuals, SMEs, or large multinational organizations. The most negative externality among the legitimate actors is created by individual users and SMEs who do by not employing risky online behavior or by not employing security measures during transactions (Asghari, 2010; Mannan & van Oorschot, 2008).

- **Security Guardians**

They are the most important actors of this system as they improve the existing banking system and help in removing the vulnerabilities and development of systems so that banking frauds can be mitigated. The security guardians in case of banking sector could be the bank itself or the some third party hired by the bank in order to ensure security from such threats.

V. FRAUD, MORE THAN ONE WAY TO LOSE

When millions of people have their credit card information stolen by hackers, it gets immediate attention. Financial crime usually involves fraud, but this can take many forms to exploit consumers, banks, and government agencies. The most damaging financial crimes penetrate
bank networks, with cybercriminals gaining access to accounts and siphoning out money. High profile cyber heists that steal tens of millions of dollars from banks are a global phenomenon. Retailers are a favorite target for cybercriminals. UK retailers reportedly lost more than $850 million in 2013. Large-scale attacks have occurred against retailers, hotel chains, an airline, and financial service companies in Australia, with losses averaging over $100 million per company. Stolen personally identifiable information and credit card data are hard to monetize, but cybercriminals are getting better at this. Since there is little risk of punishment for the hackers, this kind of cybercrime will increase.

The Financial system (FS) sector is particularly exposed to certain types of economic crime and faces unique regulatory challenges as a result.

Credit card Fraud

A major kind of electronic crime is “credit card fraud”. FS sector is presented new innovations against counterfeiting and fraud, which are highly sophisticated to profiting from or beating these systems. Most of the credit card fraud is committed with the use of counterfeited cards. Credit card fraud is also called as “Identity Theft” in which a person may use the identity of another person for exercising fraud or deception. Credit card fraud in banking sector can be committed as:

- Use of unauthorized account or personal information to consider as an act of criminal deception.
- Illegal or unauthorized use of account for personal gain.
- Misrepresentation of account information to obtain services.

For this reasons are introduced some security measures to reduce the credit card fraud but exits other part that makes difficult to eliminate this type of economic type. For this reason, the problem of credit card fraud is serious and occurring by stealing the cards and the accompanying information at the time of transaction delivery.

ATM’s Frauds

Over the past three decades, large number of banking customers depends on the ATM to conveniently meeting their banking needs. In the recent years, there have been a large number of accidents of ATM’s frauds. It is necessary to manage the risk associated with ATM fraud as well as reduced its impact on the important issues. The prevailing contemporary era has replaced long-established monetary instruments from a paper and metal based currency to “plastic money” in the form of credit cards, debit cards, etc. This has resulted in the escalating utilize of ATM all over the world. The use of ATM is not only safe and sound but also suitable. This safety and convenience, has an evil side which is reflected in the form of “ATM FRAUDS” that is an international problem. The use of plastic money is increasing for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, traveling bills and even petrol bills. The convenience and safety that credit cards carry with its use has been instrumental in increasing both credit card volumes and usage. This growth is not only in positive use of the same but as well as the negative use of the same. The world at large is struggling to increase the convenience and safety on the one hand and to reduce it misuse on the other. A few of the accepted techniques used to carry out ATM crime in banks are:

1. ATM’s card reader is tampered with in order to trap a customer’s card through card jamming.
2. Card Skimming is the unlawful technique of stealing the card’s security information from the card’s magnetic stripe.
3. Card Swapping, is another technique in which customer’s card is swapped with another card without the knowledge of cardholder.
4. Website Spoofing, here a fresh fabricated site is prepared which looks valid to the user and customers are asked to give their card number PIN and other information, which are used to reproduce the card for use at an ATM.
5. ATM machine is physical attacked for removing the cash.

Money laundering

Money laundering continues to be a hot topic in the FS sector. It is also distinct from other types of economic crime in that an FS organization does not suffer direct financial loss through money laundering – instead, the effects are felt through a loss of reputation (in the eyes of both the public and the regulator), and increasingly compounded by colossal regulatory fines. At least 50% of FS respondents in Western Europe and Africa selected money laundering as their highest risk in doing business globally, compared to bribery and corruption and anti-competition law. FS reported feeling particularly concerned about the impact of money laundering on their reputation (more so than operational disruptions or financial loss). 29% of FS respondents felt that the most severe impact of money laundering is on their organization’s reputation.

What can you do?

Ensure that “Know Your Customer” procedures and Anti-Money Laundering processes are operating effectively across a “single customer view” – making sure all relevant systems and records are joined up for consistency of data.

Resolve legacy IT issues in order to keep pace with regulatory requirements and new tactics of money laundering syndicates.

VI. DEALING WITH BRIBERY AND CORRUPTION ABROAD

Of the FS surveyed, 47% currently have operations in a market with high corruption risk. At the same time, for each associated economic crime like bribery and corruption,
money laundering and anti-competition law, around 40% of FS respondents were unable to provide an estimate of the financial loss suffered as a result. In the UK, the Bribery Act emphasizes personal liability of board members, while the 2013 Financial Services Act places the burden of proof on the individual (to demonstrate that reasonable steps have been taken to avoid bribery and corruption).

What can you do?

- Carry out risk assessments for fraud, bribery and corruption in order to identify ways of improving the effectiveness of fraud detection mechanisms as well as to mitigate the risk of regulatory breach when operating in a territory with heightened corruption risk.
- Implement comprehensive due diligence programmes on third parties which would help to highlight potential “red flags” indicating vulnerability to bribery or corruption. These red flags may include issues such as engagement with Politically Exposed Persons, negative references in media or involvement in litigation.

VII. FINANCIAL SERVICES ECONOMIC CRIME TODAY

Around half of the FS (Financial Services) respondents who have experienced economic crime during the survey period report an increase in the number of occurrences and the financial value of economic crime during the period (more so than other industries’ respondents). There are regional variations – in Asia Pacific at least half of FS respondents reported an increase; in contrast, nearly 40% of FS respondents from South & Central America reported a decrease.

Similarly, only 41% of FS respondents believe it is likely that they will experience cybercrime in the next 24 months (including some 45% in Africa and 36% in Asia Pacific). This compares to 26% in other industries. A further 19% of FS respondents are unsure whether they are likely or unlikely to experience cybercrime.

VIII. IMPACT OF CYBERCRIME ON BANK’S FINANCES

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions. The banking sector is forced to evaluate its current practices in order to analyze and manage their risks effectively. Technology driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible.

However, this has also increased the risk of becoming targets of cyber attacks. Cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and
access important business information which indirect impacts the bank's finances. Globally, USD 114 Billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double i.e. USD 274 billion (Symantec Cyber Crime Report, 2012). On an average, banking facilities take 10 days to fully recover from a cyber act which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. USD 4 billion is lost in recovering from the crime and USD 3.6 billion is spent to combat such crimes from happening in future. The average time taken to resolve the crime in Indian banking sector is also higher in comparison to global scenario.

In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organizations so that a model can be developed which can help in controlling and dealing with such threats. The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks.

High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9 million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to UK, in US as well such attacks have surfaced in the past years and in order to curb the affect, they launched the program Quantum Dawn 2 which test the efficacy of system installed in banks in response to cyber-attacks.

However, the sad truth is that most the systems are one-step behind the tools adopted by cyber criminals which has resulted in demand of development of system which is flexible is meeting and destroying the incoming assaults. A solid defense system to resolve attack is the need of the hour before, during and after the attack.

IX. CONCLUSION

The paper gives a brief overview of cybercrime scenario in the banking sector and impact of cybercrimes on bank finances. The major cybercrimes which plague the banking sector are ATM frauds, Denial of Service, Credit Card frauds, phishing, etc. These crimes are not harmless; they are causing banks financial loss which would ultimately have an adverse effect on the economy. The rapid growth to global electronic crime and the complexity of its investigation requires a global presence. Presently, the measures undertaken the banks are not sufficient and therefore it is imperative to increase cooperation among the banks across the world for the development of tools and models which can be applied to counter global banking cybercrimes.

REFERENCES