CU Global Management Review
Volume 5, Issue 2, July-December 2016, pp. 56-71

Cyber Scavenging: A Grave Threat to Financial Sector

■ **Dr Hitesh Keserwani,** Assistant Professor, Amity Business School, Amity University, Lucknow

Abstract

The financial sector is facing the highest number of organized cyber attacks and multi-channel threats. According to the latest Threat Metrix Cybercrime Report (2015) more than 15 billion transactions in the past 12 months revealed a 40% increase in cyber criminal activity targeting the financial sector. A record 21 million fraud attacks and 45 million bot attacks were detected in the last three months of 2015. The ease of online banking and transactions has brought a significant rise in malicious attacks and these cyber-attacks continue to hit financial institutions. Consequently, these institutions suffer a loss of brand image, customer faith and regulatory issues etc. A report by Arbor Networks reveals that 2013 witnessed a huge rise in cyber-attacks in the banking and financial service sector. In India the attack against financial institutions and government organizations are registered as 34% and 43% respectively in 2013. In 2014, cyber thefts and attacks increased by 15% and 19% respectively, the report revealed. Another survey conducted by The Depository Trust & Clearing Corporation (DTCC, 2014) states that twenty-four per-cent of respondents, which comprised of broker-dealers, banks, mutual funds, insurers and hedge funds, said cyber-threats were the biggest risk for the broader economy, while 23% said it was the largest risk to their firm. With a growing percentage of risks and loss to financial institutions, companies of all sizes need to re-examine, re-think and possibly re-architect their security posture. Therefore there is a great desire to stay ahead of the accelerating cyber-crime and need to proactively comply with evolving government regulation. The study critically examines the existing infrastructure and techniques used by these financial institutions and suggests them a robust framework to mitigate the evolving challenges and also a control mechanism to reduce the increasing percentage of cyber threat year after year.

Keywords: financial institution, economy, cyber threat, criminals, regulations.

Introduction

Internet banking enables customers to save time, take control of their personal finances and even help the environment by opting to receive electronic statements. For Internet banking users,

online banking services are the most important driver of financial institution selection, falling just behind rates/fees and customer service. These days, it's not good enough to simply offer online banking services, however. To maintain existing customers and attract new ones, financial institutions need to keep their offerings up to date with the latest features. Who are these customers? In a nutshell, they are younger, wealthier and more desirable than the average banking customer. Financial institutions must ensure the capabilities of their Internet Banking Solution that can proficiently deliver on these customer needs, especially as younger customers gain more and more financial responsibility. Online banking doesn't just appeal to the young consumers; it appeals to the more educated and affluent segments of the population as well. Non-online bankers value a personal relationship with their financial institution, and they place high importance on service offerings that can be expensive which further motivates the customer to turn into online banking platform.

The Indispensible Internet Banking

For financial institutions, Internet banking offers a myriad of direct benefits. Online bankers conduct transactions faster and more easily with 24/7 self-service applications. This not only makes the institution more valuable to customers and also reduces operational costs in terms of time and money. For instance, a face-to-face transaction with a teller costs financial institutions considerably more manual labor and paper, than an online transaction. Internet banking further reduces costs by decreasing lobby traffic, cost savings customer phone calls and the need to print and mail paper statements. With a fully integrated Internet Banking Solution, financial institutions can optimize internal systems and processes, provide a comprehensive view of financial activity for users and easily integrate additional capabilities. By reinforcing the online offerings with quality service and support, financial institutions can further improve customer relationships and benefit from an increase in overall profitability. While nearly every online banking solution offers some functionality to enhance convenience, control and cost savings, there are a number of key features customers seek that many older systems do not offer. Filling those gaps is critical to financial institutions looking to remain competitive.

Customers are looking for added functionality in multiple areas however several system enhancements are desirable to increase customer control over their finances via online banking. One major example is the ability to conduct inter-institution money transfers. Financial institutions have enhanced transfer functionality with cross-institution aggregation, enabling customers to consolidate their financial information and more efficiently manage funds.

Customers increasingly want to tailor their online banking experience for simplicity and control, and an important enabler is the ability to set up e-mail alerts. With the latest Internet

Banking Solutions, online customers can sign up for billing e-mail alerts that automatically inform them when a payment is due or has been made. Additionally, customers can set up alerts to notify them of activities like money transfers, deposits, balance falling below a predetermined level, changes to personal information or any unusual transaction.

To further meet demands for enhanced account management, financial institutions can give customers more control over their finances with a solution that integrates personal financial management (PFM) capabilities. Effective PFM delivers the features that customers find most valuable for managing their funds.

Internet Banking Solution: Customized for Customers

With the right Internet Banking Solution, financial institutions can alleviate the limitations and challenges they are experiencing with their current system. In effect, the institution can save significant time and money, while greatly reducing the risk of losing valuable customers due to an inadequate solution. For many small- and mid-sized financial institutions, an outsourced solution makes the most sense. Excellent, ready-made options are available to enable these institutions to offer the functionality their customers demand without expensive internal development and ongoing maintenance requirements. An outsourced solution not only reduces costs, but also increases flexibility and security.

The first criterion when researching an outsourced solution should be high availability of resources. An optimal solution will also include a call center for account holders to easily contact with questions or concerns. While most Internet banking providers expect financial institutions to take their own calls, some providers offer post-conversion, 24/7 customer support directly to the institution's customers. Financial institutions typically choose the duration that the provider operates this call center, which may be as brief as six months.

Features and functionality are the next most important decision criteria. Before selecting a provider, the financial institution should have a solid understanding of their "must have" functionality. Assessing vendors based on the breadth of their offerings is critical. It's not enough to simply check off the specific features that are being sought. Financial institutions need to understand a potential vendor's recent product enhancements, as well as their product roadmap. Financial institutions must be sure to select a partner that will move them forward as customer needs and technology evolves.

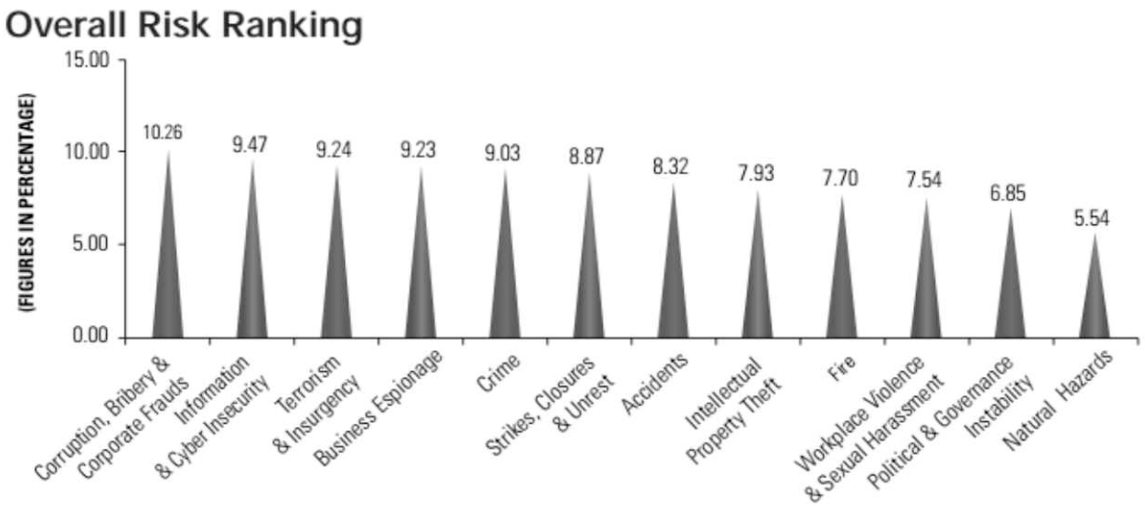
Technology: The biggest boon for Financial Sector

In financial domain, technology is no longer an enabler, but a business driver. In last decade phenomenal growth of IT, mobile penetration and communication network has facilitated

growth in extending financial services to masses. Technology has facilitated delivery of banking services to masses and changed the way of functioning of financial institutions. Technology made banking services affordable and accessible by optimizing the way these institutions operate today. Regulatory bodies, banks and other institutions/agencies have taken paradigm shift in areas of respective operations, service delivery and consumer satisfaction. Financial institutions gained efficiency, outreach, spread through technology in last two decades.

The benefits of technology such as scale, speed and low error rate are also reflecting in the performance, productivity and profitability of banks, which have improved tremendously in the past decade. Technology initiatives are taken by banks in the areas of financial inclusion, mobile banking, electronic payments, IT implementation and management, managing IT risk, internal effectiveness, CRM initiatives and business innovation.

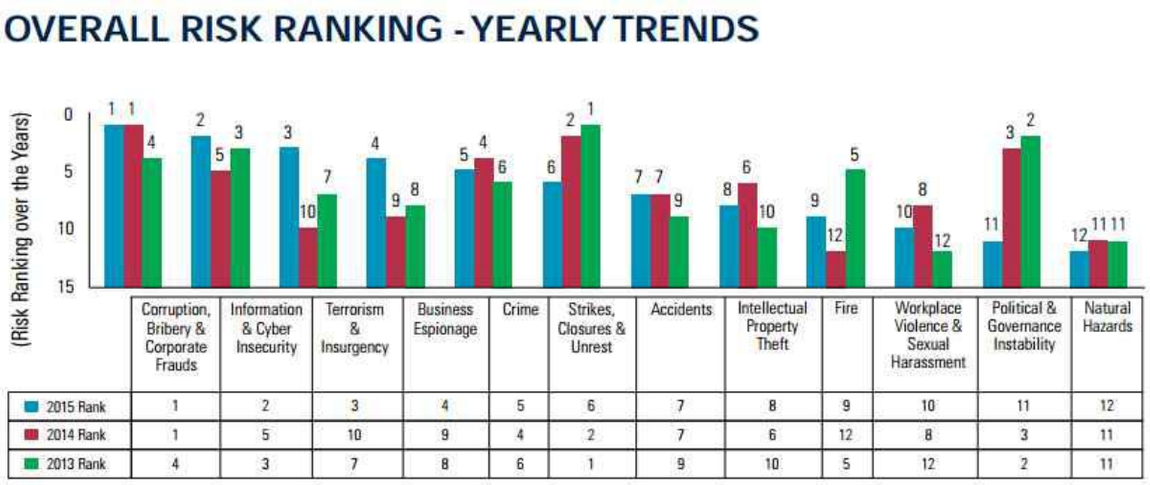
FIGURE1. OVERALL RANKING OF RISK IN INDIA



Source: India Risk Survey 2015

- The figure 1 India Risk Survey 2015 (IRS 2015) attempts to showcase the views and perceptions of key business leaders, public figures, as well as professionals across various sectors and geographies regarding operational, safety and strategic risks. Information security is a growing concern with increasing technological advancements and the tendency of corporate houses to create more and more intellectual property and competitive strategies any compromise with the network would be providing an opportunity for frauds and the corporate to stand at risk which in turn will incur unimaginable losses.

Figure2. Overall risk ranking – Yearly Trends



Source: India Risk Survey 2015

The figure 2 clearly states that information and cyber insecurity is on rise in India and stands in second position after third in 2013 and fifth in 2014 which is alarming and biggest hurdle in the development of the country because in this digital age, where online communication has become the norm, internet users, governments and organizations face increased risks of becoming the targets of cyber-attacks. As cyber criminals continue to develop and advance their techniques, they are also shifting their targets — focusing less on theft of financial information and more on business espionage and accessing business information. To fight fast-spreading cyber-crime, sector must collaborate globally to develop an effective model that will control the threat.

Increasing Cyber threat: A grave challenge for Financial Institutions

Financial-services organization provides specialized, private banking products and services to its customers. Its services cover property, investments, capital markets and asset management. Their customer base is its biggest asset, and offering strong protection to these customers is of paramount importance – both to retain and grow business, and to protect its reputation for high-quality service. Companies in financial domain have experienced increase in instances of cybercrime in past few years. Various levels of cyber-crime threats are at each level of IT systems. The emergence of such threats at different levels is due to an explosion of online

banking and shopping, coupled with the increasing willingness of consumers to disclose personal information over the internet. Hackers are now enabling a larger market of 'script-junkies' whose deficient skills would otherwise shut them out of the cyber-criminal enterprise.

According to the report (Symantec Cyber Crime Report, 2011) the survey conducted under the report highlights the issues of primary importance as no national government operates an effective compilation service to identify trends in cyber-crime with the exception of the Internet Crime Complaint Center (IC3). Most cyber-crime is on such a small scale that law enforcement organizations are not interested in dealing with individual cases, and, in many cases, individuals may not care enough about the amounts involved to take action. Therefore it tends to go unreported.

Indian Scenario

USD 4 billion is the total loss of cash in 12 months

USD 3.6 billion is the total loss of time for victims of cyber crime

On an average 15 days were spent by victims to satisfactorily resolve hassles of cyber-crime.

Threat

Among all cybercrime victims surveyed 80 percent were from emerging markets, compared to 64 percent in developed markets.

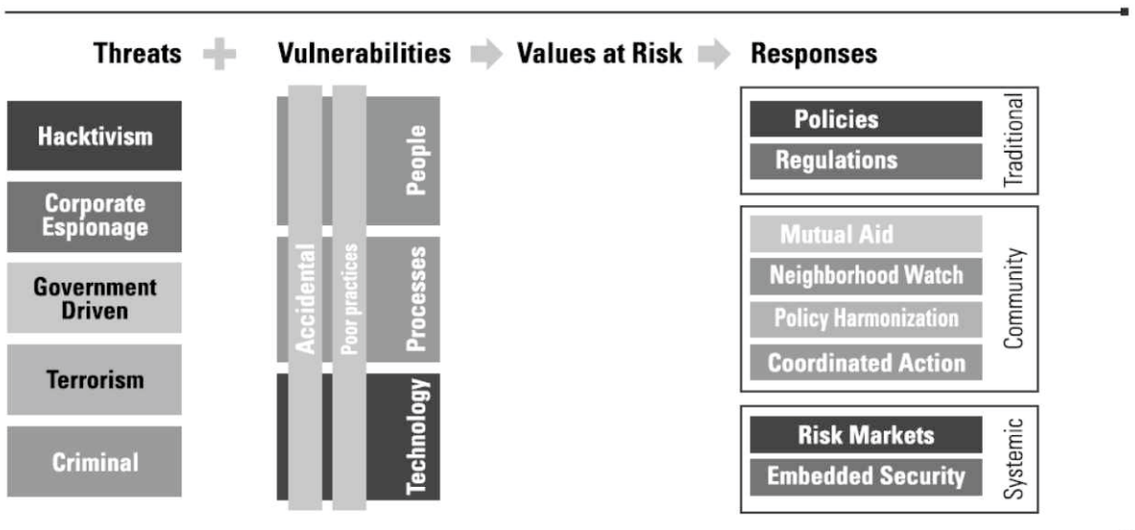
Only 21percent of victims reported cybercrime to the police

59 percent of victims who'd suffered both online and offline crime felt there were fewer ways to get help after the cybercrime

In India, 59 percent of mobile phone owners access internet via mobile device out of which 17 percent experienced mobile related cyber-crime.

According to the (World Economic Forum Report: Global Risks 2012) Vendors of online security products have an interest in talking up the threats of cybercrime, while victims of cybercrime often have an interest in remaining silent. It is therefore very difficult for firms and organizations to get a clear picture of the true levels of the risk and needs for investment. Correcting such information asymmetries should be at the centre of policies to improve global cyber security and to ensure an efficient market. Firms have an incentive to invest in cyber security measures that protect their own interests, rather than in those measures that contribute to the health of the overarching critical information infrastructure. Innovative multi stakeholder collaboration will be required to tip the balance towards investment in creating systemic resilience.

Figure 3: Framework of Cyber threats in Indian Financial Institutions



Source: World Economic Forum Report-Global Risks 2012 Seventh-edition

- The Figure 3 clearly states that Cyber-crime has spawned many entrepreneurs, though of dubious repute. They have given rise to new criminal hacking enterprises aimed not at committing fraud but at providing services to help others commit fraud. This operation enables people to commit crime vicariously, i.e. without any direct perpetration.

Another model is to create a subscription based identity theft service rather than stealing personal credentials themselves cyber criminals have hacked into PCs and then charged clients for a limited period of unfettered access. As is the case with most business services, customers willing to pay extra can obtain premium services such as a complete 'clean-up' of the stolen data, i.e. getting rid of low-value information and assistance with indexation and tagging of data, etc. New skills, technologies and investigative techniques, applied in a global context, are required to detect, prevent and respond to cyber-crime. This is not just about the realignment of existing effort. This 'new business' will be characterized by new forms of crime, a far broader scope and scale of offence and victimization, the need to respond in a much more timely way, and challenging technical and legal complexities. Innovative responses such as the creation of 'cyber-cops' ,'cyber-courts' and 'cyber-judges' may eventually be required to overcome the significant jurisdictional issues that law and order agencies are currently facing. Law enforcement with regard to investigating crimes and handling evidence, dealing with offenders, and assisting victims, poses complex new challenges. There is an unprecedented need for

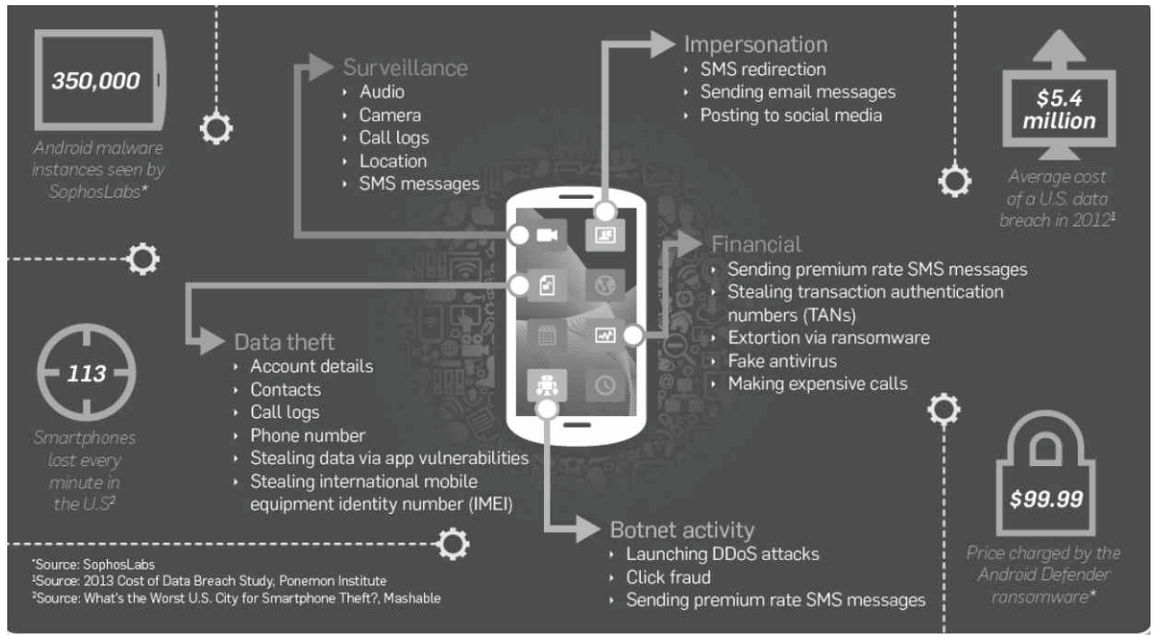
international commitment, coordination and cooperation since cyber-crime is truly a global phenomenon. It is also important to have a better understanding about the nature of the problem and to address the issue of significant under-reporting of this dangerous phenomenon. Prevention and partnerships will be essential to fight cyber-crime.

Cyber security is on top priority list of various financial organizations, regulators and governments. Cyber-attacks ranked fourth in top global risks in terms of likelihood in World Economic Forum Report: Global Risks 2012.

Smart phone usage: An additional Treat

With the increasing usage of mobile in financial services Your Android smartphone may become dangerous when compromised by malware, it can illegally watch and impersonate you, participate in dangerous botnet activities, capture your personal data, and even steal your money.

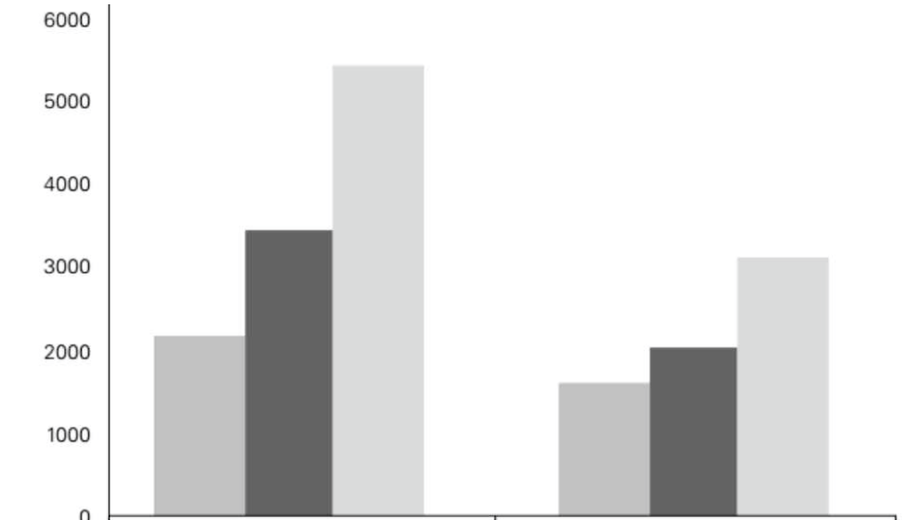
Figure 4: Smart phone usage and rising risk



Source: 2013 cost of Data Breach Study, Ponemon Institute

The Figure 4 states that Majority of the banks in India have migrated to online and mobile banking. Most of the transactions are conducted via payment cards, debit and credit cards, and electronic channels such as ATMs. Consequently, both private and public banks, as well as financial institutions in India are becoming increasingly vulnerable to sophisticated cyber-attacks. As per the Internet Security Threat Report 2014 by Symantec global survey of end-users, 38 per cent of mobile users had already experienced mobile cyber crime.

Figure 5: IT Crimes registered in India under IT Act (2008) and IPC



	Cases Registered	Persons Arrested
2011	2171	1592
2012	3405	2004
2013	5370	3074

Source: 2013 NCRB Report, India risk survey 2015.

As per the NCRB 2013 Report a total of 5,370 cases were registered under the IT Act and IPC during 2013 as compared to 3,405 cases during the previous year (2012), thus showing an increase of 57.7 per cent in 2013 over 2012. As per available data, India ranks 3rd after the USA and Japan when accounted for the risk of being affected by online banking malware, with majority of the instances being attributed to phishing and debit / credit card frauds.

According to Fifty-second report standing committee on Information technology (2013-14) the total number of websites defaced/hacked during the last five years:-

Table 1: Number of Indian and worldwide websites hacked

Numbers of Indian and world-wide websites defaced / hacked		2008	2009	2010	2011	2012	2013 (upto February)
World wide	Websites defaced/hacked	517459	544409	1419202	1612728	1274162	Data not yet available
	Government/ Strategic Organisations' websites defaced/hacked	9606	11929	16875	Data not available	Data not yet available	Data not yet available
India	Websites defaced/hacked	6310	12161	20701	21699	27605	3911*
	Government websites defaced/hacked	90	201	303	308	371	40*

* *Upto June 2013 the no. of total Websites defaced/hacked was 12693, of which Government websites are 78 and other 12615*

Source: Fifty-second report standing committee on Information technology (2013-14).

Cyber criminals are forming private, trusted, and organized groups to conduct cyber-crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber-crime by providing actors of all technical abilities with the necessary tools and resources to conduct cyber-crime. Not only are criminals advancing their abilities to attack a system remotely, but they are becoming adept at tricking victims into compromising their own systems. Once a system is compromised, cyber criminals will use their accesses to obtain PII, which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cyber-crime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement.

The potential economic consequences are severe. The sting of a cyber-crime is not felt equally across the board. A small company may not be able to survive even one significant cyber-attack. On the other hand, companies may not even realize that they have been victimized by cyber criminals until weeks, maybe even months later. Victim companies range in size and industry.

Often, business groups are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been

compromised, so they absorb the loss, making it impossible to accurately calculate damages.

The Fifty-second report standing committee on Information technology (2013-14) discusses about financial loss to the country due to cyber-attack/fraud in last five years, according to Reserve Bank of India (RBI), the number of fraud cases as reported by Banks on account of ATM Debit Cards / Credit Cards / Internet have decreased from 15018 (in 2010) to 8322 (in 2012). However, the amount involved had increased from Rs. 40.48 crore in the year 2010 to Rs. 52.66 crore in the year 2012. Central Bureau of Investigation (CBI) has also registered cases pertaining to financial frauds under the provisions of Information Technology Act 2000 along with other Acts which are as follows:-

Table 2: Financial loss to the country from 2010 to 2012

Year	No. of Cases	Amount Involved in Crore (Rs. In crore)
2010	6	6.42
2011	10	12.43
2012	8	28.79

Source: KPMG India Fraud Survey 2012.

According to KPMG India Fraud Survey 2012 financial services as being the most vulnerable to fraud, whether it is known frauds such as bribery and corruption, or emerging frauds that are technology dependent such as internet banking and mobile banking frauds. Financial sector frauds are becoming complex, their incidence geographically wide spread – many a time perpetrators of internet based frauds and data theft are outside the jurisdictions where fraud is committed – and the quantum of fraud rising.

With greater technology integration in the financial services sector, there are greater challenges. New service delivery platforms like mobile and social media are becoming interfaces between financial institutions and customers, revolutionizing the way financial services are delivered. However, with these new platforms comes the challenge of providing a secure environment for customers to conduct transactions. Hostile software programs or malware attacks, risks of phishing, Vishing (voicemail), SMSishing (text messages), Whaling (targeted phishing on High Networth Individuals) and theft of confidential data are all real threats if a secure environment is not established. Additionally, money laundering and terrorist financing (ML/TF), and tax evasion are also issues plaguing the financial services sector.

Financial Regulations: Steps in mitigating evolving threat to Indian financial institution

- Recent FATF34 recommendations indicate that Indian firms would have to set up a comprehensive framework for compliance that includes identification of beneficial ownership and key influencers for an entity. This will also increase the levels of monitoring, diligence and remediation activities carried out by the sector.
- Other regulations like the Dodd-Frank Act which prohibits banking entities from any transaction or activity that may involve or result in a material conflict of interest for banking entities, or Foreign Account Tax Compliance Act (FATCA) that prevent offshore tax evasions by US citizens with extra-territorial jurisdiction, are being enforced, which will impact Indian financial institutions even as they grapple to understand these laws.
- From a regulatory perspective, Indian regulators such as RBI, IRDA and SEBI have been tightening scrutiny and increasing enforcement. In recent years 46 banks being fined for non-compliance to AML requirements and insurance companies were being fined by IRDA for violation of norms relating to payment of commissions to corporate agents and brokers. SEBI has also set up a Forensic Accounting Cell to investigate potential market manipulation issues. This detailed scrutiny is expected to continue and one can see higher number of sanctions and hefty fines for non-compliance.

International best practices: Suggestive measures for financial institutions to mitigate the increasing risks

- Conducting yearly risk assessments to identify potential fraud risk prone areas and developing specialized financial crime prevention skills to deter frauds. This should consider global compliance requirements also.
- Employees should be trained and equipped with relevant skills and knowledge about recent fraud modus operandi. They must also be informed of whistleblower channels available to them to report any instances of fraud, misconduct and non-compliance.
- Monitoring channels like social media to gather intelligence and act on early warning signs
- Building an effective Know Your Customer (KYC) framework to prevent any abuse of customer rights and fraudulent transactions.

Financial Fraud Management: Future Trends

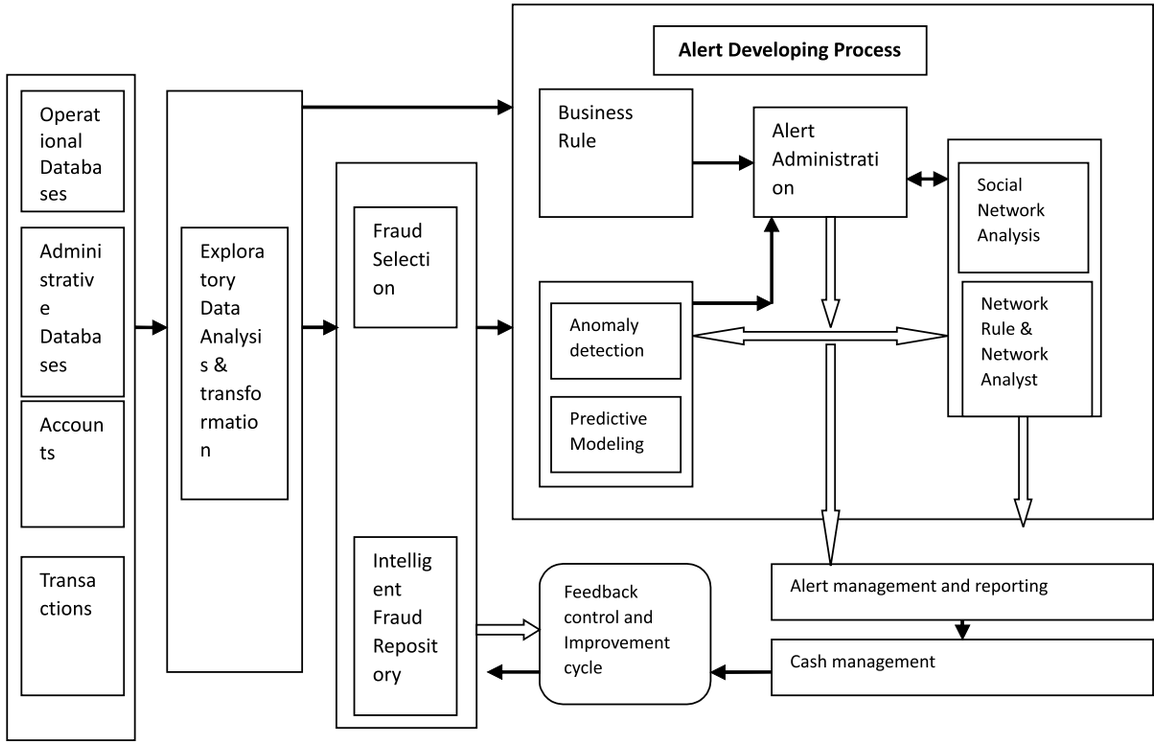
To more effectively prevent future losses, fraud management systems will have to become self-learning, and adaptable to a dynamic environment and evolving fraud techniques. Financial

institutions already can seamlessly test the effectiveness of fraud-detection rules and models – and update them when test reports indicate the need. Ideally though, the system would automatically capture the outcomes of investigations and reuse those outcomes in future scoring. Models would thereby adapt readily to new knowledge and continually be refined. Auto-generated network diagrams would enable strategists to see patterns and symptoms that lead to improved controls and new monitoring techniques.

This combination of adaptation and visibility would enable financial institutions to better understand emerging threats so they can take action to prevent substantial losses before they happen.

The prospects for the future also extend beyond the scope of any single enterprise. As more organizations adopt integrated, automated fraud management systems, the potential is there to create a broad consortium of financial institutions that can draw on their collective experiences to improve fraud detection across the industry.

Figure 6. Indian financial Institutions: A Proposed Framework to mitigate evolving online threats



The above framework would help the Indian financial institutions to mitigate the online risk with the help of analytical modeling tools and specialized databases. Data gathered from the operational databases are updated to OLAP (Online analytical Processing system) which further facilitate the financial institution to perform mining to their specialized databases and identify the hidden patterns of fraudulent acts that helps them to device a methodology in order to control the suspicious or fake transactions by alert system. Also with the integrated system and high end data analytics, predictive modeling will become much easier which would definitely be a great help in risk estimation and forecasting.

Conclusion

In the current technological environment, there are numerous threats to private sector networks, and the current Internet environment can make it extremely difficult to determine attribution.

Regulatory bodies and financial institutions are optimistic by strengthening relationships with both domestic and international counterparts; the RBI will continue to succeed in identifying and neutralizing cyber criminals, thereby protecting Indian businesses and critical infrastructure from grave harm.

To bolster the efforts in minimizing security risks, it is important that private institutions to continue to share information with government agencies with applicable laws and policies and also continue to engage in strategy discussions with other government agencies and the private sector to ensure that Indian ingenuity will lead to new solutions and better security. Another important aspect is to continue to build a skilled workforce to operate in this challenging environment.

It is therefore the effort should be made in the collaboration with RBI and Security agencies as a whole to determine a successful course forward for the nation that allows us to reap the positive economic and social benefits of the Internet while minimizing the risk posed by those who would use it for nefarious purposes.

References:

Business standard, July 20, 2011, http://www.business standard.com /article/finance/ 7-account-holders-in-india-usa-net-banking-study-111072000193 1.html//accessed on Aug 20,2013.

Consumers and Mobile Financial Services 2013 by BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM.

Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.

Cyber Crime – A Growing Challenge for Governments July 2011, Volume Eight kpmg.com

Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (2012) by Nina Godbole and Sunil Belapure, Wiley India Pvt. Ltd, New Delhi, India.

E-Crime Survey 2009, KPMG International

Fifteenth lok sabha Ministry of communications and information technology (department of electronics and information technology) Cyber crime, cyber security and right to privacy Fifty-second report (pp 3-5).

French K et al. 2010. The Squam Lake Report: Fixing the Financial System. Princeton: hhtp://omgtoptens.com/misc/business/top-10-banks-that provide-best-internet-banking facilities india /accessed on Aug 20,2013

Indian Risk Survey 2015- http://ficci.in/Sedocument/20328/India-Risk-Survey-2015.pdf.

KPMG in India: IT in Banking Managing the present by looking to the future, August 2008.

KPMG international, Issues Monitor: Cyber Crime – A Growing Challenge for Governments (July 2011, Volume Eight)

Litan, Avivah. Gartner Research. Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations. May 2008.

MOBILE APPS FOR BANKING Benchmarking Best Practices Strategies by my private banking research April 2013.

Princeton University Press. 168 pp. REPORT ON TREND AND PROGRESS OF BANKING IN INDIA 2012-13 Research, Vol.3, December 2003.

The state of financial Trojan (2013) by Stephen Doherty, Piotr Krysiuk, Candid Wueest Version 1.02 – December 17, 2013.

Trend Micro's 2014 Threat Round Up Report - http://gadgets.ndtv.com/internet/news/india-third-most- affected-by-online-banking-malware-report-543205

Vij Madhu, "The New World of Banking: A Paradigm shift", Journal of Management World Economic Forum Report: Global Risks 2012

Volume 5, Issue 2, July-December 2016, Print-ISSN 2349-1078