CYBER RISK IN E-BANKING

Dr. Lalitha.B.S.
Associate Professor
School of Commerce
Jain Group of Institutions
Bangalore
India

Abstract: In the olden days the bank's aim was purpose oriented, but gradually it has become customer oriented. Innovation has become the buzz of the day. Each day throws up a new challenge and it has become increasingly difficult for the banks to retain their customers unless they offer safe, secure services. Services like ATM, Internet Banking, Mobile Banking have been introduced by the banks. Demonetization wave of November 2016 augmented the usage of these services. But these services brought in a range of fresh problems also to the banking industry. This article tries to highlight the latest strategies adopted by the Government and the RBI to combat these cyber attacks.

Keywords: ATM, Internet Banking, Mobile Banking, Cyber frauds, RBI Initiatives

Introduction: Indian banking industry has witnessed a paradigm shift in its working when compared to how banks functioned in 1960-1990s. In the present scenario customer's expectations, technological capabilities, regulatory requirements, demographics have created a crucial change in the banking industry. Banks need to go ahead and adopt a positive approach to the security of customer information. Particularly after demonetization in India, there is a noticeable shift in the mindset of the customers to deal with electronic form of transactions. There is a rapid usage of digital channels such as internet banking, mobile banking, card based payments and ATM (Automated Teller Machine). Gradually India is shifting toward a cashless economy. The exponential growth towards digital payments in India and the strong push towards a cashless economy have renewed focus to the need to strengthen financial security. Banks have tried hard to enhance the services through these different channels to its customers. These channels have decreased the time, cost and the effort involved in completion of the transaction. But at the same time, these channels have led to the leakage of customer's information.

Banks and financial institutions are more vulnerable to cyber attacks and online frauds. Surprisingly Indian banks ranks third in the financial Trojan infections and has witnessed a six fold increase in debit card and credit card fraud cases in the past few years. Cyber attacks against the financial system have become sophisticated, repeated and unpredictable. With the increased severity of the attack, a resilient and flexible cyber security model only can help financial services companies to survive the inevitable risk. Cyber criminals are finding out new ways to gain access to customer's bank account information. Cyber attacks have become increasingly diverse and unpredictable. This has decreased the customer's confidence and trust which creates a serious impact.

In June 2016, RBI (Reserve Bank of India) has mandated all banks to put a cyber security policy which contains an appropriate approach to combat cyber threats and ensure adequate cyber security preparedness on a continual basis. RBI has pointed out that the numbers, frequency and impact of cyber attacks on Indian banks have increased substantially. Indian banks are committed to maintaining customer trust, protecting financial assets and preserving their own brand and reputation like their global peers. Thus there is an urgent need to improve cyber defense in the country. The present mandate of the RBI is considered as timely and essential to build a strong and robust banking system in the country.

Meaning of cyber attack: According to the PwC's (Price Water Coopers) Global Economic Crime Survey 2016, cyber crime is the second most reported crime across the globe. A cyber attack can be defined as a manoveure engaged by individuals or organizations that target computer information systems, computer

networks or personal devices or by various means of malicious acts usually that originates from an anonymous source that steals, alters and destroys a specified target by hacking into a susceptible system. This act maybe confined to the organization or from remote locations via the internet.

Recent global cyber attack trends: The number /figures of cyber attacks have increased significantly in the country and across the globe. Individuals, businesses and organizations are the worst affected from such attacks. The profile and the motivation of the cyber attackers are fast changing. Some of the recent financial attacks in the world are as follows:

a. In 2015, Vietnam's Tien Phong Bank interrupted an attempt to use fraudulent messages to initiate fund transfers like the SWIFT (Society for Worldwide Interbank Financial Telecommunication) and the same methodology was later used in the Bangladesh bank case.
b. In January 2016, Ecuador's Banco Del Austro SA sent messages over the Swift system instructing Wells Fargo and Co, to transfer US $12 million, but the bank has understood that to be the work of cyber criminals according to Reuters.
c. Europe's largest lender HSBC was also prone to DDoS(Distributed denial of service) cyber attack in January 2016 leaving thousands of customers unable to access their accounts.
d. In February 2016, hackers claimed luck at Bangladesh Bank. A customized software which acted as a connecting link between the bank system and the central SWIFT infrastructure was targeted. Cyber thieves had instructed to transfer an amount of US$951 million out of Bangladesh's banks account to the New York Federal Reserve. Majority of the transactions tragedy were averted, but the cyber attackers made US $81 million into their pockets.
e. In August 2016, Bitfinex, a Hong Kong exchange of digital currencies announced that some of the customers' accounts were hacked and bit coins worth of US$ 65 million were stolen. This reduced the customer's trust towards the bit coins.
f. India too faced a similar attempt by generating fraudulent payment instructions on the Nostro accounts and transmitting them over SWIFT messaging system. Continuous follow up with the paying banks prevented the monetary loss. In October 2016, 32 lakh debit cards of various banks were subjected to a cyber malware attack. The following table shows the details of the various types of crimes as published by the National Crime Record Bureau

Type of case	2013	2014	2015	% Increase / Decrease in 2014 since 2013	% Increase / Decrease in 2015 since 2014
Cheating using computer as a medium or target.	-	1115	2255	-	102.2
Forgery using computer as a medium or target	747	63	45	-91.5	-28.6
Criminal breach of trust/fraud using computer as a medium or target	518	54	42	-89.6	-22.2
Counterfeiting using computer as a medium or target	59	10	12	-83.0	20.0

Source: National Crime Record Bureau

Challenges faced by the Indian banks:
1. **Severe compliance system:** Banks are compelled to implement the various regulations introduced by RBI. Over the past few years, the volume of transactions has increased dramatically in the branches. Such type of regulations impact the smaller banks when compared to the larger banks.
2. **Struggle to secure customer data:** Improper security measures have paved way for unauthorized sharing of data with third parties, loss of client's personal data, loss of card data are some of the modes in which the customer's data privacy is violated.

3. **Third party risk:** Banks need to conduct regular due diligence with the third parties they are associated with. As per the payments card industry security standards, these parties need to share any critical issues associated with the data environment in the banks.
4. **Evolving cyber threat landscape:** Latest technology has also brought in a wave of cyber threats like next generation ransom ware, web attacks and more.
5. **Transaction frauds:** Fraud detection technologies must be implemented with due importance to the risks based on the business factors.
6. **Secure SDLC (Software Development Life Cycle)**: Banks need to incorporate SDLC security for all banking products and applications.

Security Considerations for Alternate Banking Channels in India: Banks may offer sub variations in the services offered under the following alternate banking channels but the security considerations remains the same. Some of these considerations are as follows:

1. Internet Banking: Multi factor authentication, strong passwords, adaptive authentication, image authentication are to be adopted.
2. Mobile Banking: Mobile banking applications must be updated and tested. Latest hardening standards are to be adopted.
3. Wallet transactions: Awareness campaigns on phishing, malware attacks, vishing and social engineering, password security can be incorporated.
4. ATM Security: Biometrics like eye retina, voice scan, fingerprint scan should be introduced by the banks.
5. UPI (Unified Payment Infrastructure): Banks need to think on various security strategies, governance models, and predictive controls to build a secure UPI environment that ensures a seamless user experience and at the same time balances security risk.

Latest trends from Government of India and RBI Initiatives to curb cyber threats in the Indian Banking Industry:

1. Indian Computer Emergence Response Team (Cert-In) has been established to monitor Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among private and public cyber users and organizations in the country. A national Cyber coordination centre has also been established. CERT-In has also come out with National Cyber Crisis Management Plan and Cyber security Assessment Framework.
2. In 2017-18 budget the Finance Minister has also announced the establishment of dedicated Computer Emergency Response Team for the Financial Sector (Cert-Fin). This emergency team is slated to work in coordination with the financial regulators and other stakeholders.
3. Expert Panel from the industry has been framed with industry members as representatives. This team provides assistance in cyber security initiatives of banks, review examination reports and suggests actionable items.
4. RBI has proposed to set up a Cyber Security Lab to assist IT examiners in conduct of cyber security of banks. RBI is also under the process of operationalizing Reserve Bank Information Technology Private Limited (ReBIT). The ambit of ReBIT is to focus on IT systems, cyber security of the financial sector and also assist in the audit and assessment of the entities regulated by the RBI.
5. On June 2, 2016 RBI came up with a circular for banks to frame cyber security policy, to prepare a cyber crisis management plan, to make arrangement for continuance surveillance, to reckon the security aspects while procuring, connecting, implementation of the hardware, software, network devices to ensure protection of customer information, to ensure unusual cyber incidents with the RBI, to assess the gaps in cyber security preparedness and set up a Cyber Security operations centre.
5. RBI mandated all the banks to put in place a cyber security/resilence framework elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk duly approved by the board.
6. In order to address the need for the entire bank to contribute to a safe environment, cyber security policy should be distinct and separate from the broader IT policy so that it can highlight the cyber threats and measures to mitigate the same.
7. Banks need to proactively promote their customers, vendors, service providers and other relevant stakeholders an understanding of the bank's cyber resilience objectives and require to ensure appropriate

action to their synchronized implementation and testing. This helps the banks in building cyber security awareness.

8. IT(Information Technology) architecture should be designed in such a manner that it takes care of the security measure in all the times. The same must be upgraded in a phased manner.

9. Cyber attacks can occur at any time and cannot be anticipated. Hence it is mandated that a Security Operations Centre must be set up. This centre ensures continuous surveillance and keeps itself updated with the latest emerging cyber threats.

10. Connections are allowed to business or operational requirement. But if the same is not closed or blocked they are vulnerable to cyber attacks. Responsibility over such networks and databases should be clearly elucidated and invariably rest with the officials of the banks.

11. Banks depend on technology heavily not only in their smooth functioning but also in providing digital consumers and process collects various personal and sensitive information. Hence banks need to ensure that the reliability, confidentiality and integrity of the data have to be maintained.

12. Cyber Crisis Management Plan (CCMP) should be evolved to address the problems of detection, response, recovery and containment. Banks need to take effective measures to prevent cyber threats and to promptly detect any cyber intrusions so as to respond/recover.

13. Banks have been reluctant to intimate cyber incidents to RBI. Hence banks are encouraged to actively participate in the activities of CISO‘s (Chief Information Security Officer) forum coordinated by IDRBT (Institute for Development and Research in Banking Technology). Reporting of cyber incidents to Indian Banks- Center for analysis of risks and threats (IB-CART) set by IRBDT. Such collective efforts will help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures.

14. Any gaps, proposed measures/controls and their expected outcomes, milestones with timelines for implementation of the proposed measures/ controls, measurement criteria for assessing their effectiveness proposed by the bank may be submitted to the Cyber Security and Information Technology Examination Cell of Department of Banking Supervision.

Conclusion: Retail Banking can be considered as the major contributor to frauds in the banks. Over the years, cyber crime has grown in leaps and bounds causing losses to many customers. A recent KPMG (Klynveld Peat Marwick Goerdeler) report has revealed in one of its survey that cyber threats are more on the offing. It is time to scale up for cyber security and challenges. Inadequacy of resources to use updated technology, lack of knowledge and awareness on cyber fraud are some of the major problems faced by the banks. In addition to these problems, digital investigative challenges were identified coupled with lack of cyber detection tools and technologies, qualified personnel to carry on the investigation have also paved way for increase in these crimes. It may also be noted at this juncture that insufficient legislation and legal enforcement have also boosted the growth of such incidents. A bank with better cyber security offer can attract potential customers and retain existing ones. So banks will have to build a holistic, integrated fraud management to boost cyber intelligence and response. It is high time the Cyber Security Framework must be implemented in a strict and timely manner with regular audits to ensure comprehensive compliance. Banks need to invest in smart, intelligent and smart faceted solutions that can handle cyber crime threats by preempting suspicious activity across a customer’s journey at several touch points. This must also be accompanied by attempts to ensure widespread customer education and awareness.

Bibliography:

Shewanga Dzomira (2014) " Electronic fraud(Cyber fraud) risk in the banking industry, Zimbabwe" Risk Governance and Control : Financial Markets and Institutions , Volume 4, Issue 2

Sultana Sharmeen Karim (2016) " Cyber crime scenario in banking sector of Bangladesh : An overview" The Cost and Management Volume-44, Number-2, March-April

Reports Referred:

Deloitte Report (2016)- Cyber Security De-Risking India's Banking Industry

Information Technology and Cyber Risk in Banking Sector- The Emerging Fault lines- Keynote address By Shri.S.S. Mundra, Deputy Governor, RBI at the " International Serminar of Cyber Risk and Mitigation for Banks" organized by CAFRAL in Mumbai on Sep.7, 2016

RBI's notification on Cyber Security Framework in Banks dated June 2, 2016

Websites referred:

www.bdo.in

https://www.medianama.com/2017/04/223-rbi-cyber-crime-fraud/

https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html