S S Mundra: Information technology and cyber risk in banking sector – the emerging fault lines

Keynote address by Mr S S Mundra, Deputy Governor of the Reserve Bank of India, at the "International Seminar on Cyber Risk and Mitigation for banks", organized by the Centre for Advanced Financial Research and Learning (CAFRAL), Mumbai, 7 September 2016.

* * *

Assistance provided by Shri R Ravikumar is gratefully acknowledged.

Good Morning!

1. At the outset, I would like to compliment CAFRAL for organizing this International Seminar on Cyber Risk and Mitigation for banks and FIs, a topic which has assumed centre stage, not only in India but globally. Let me begin by quoting John Chambers, former CEO of CISCO, who famously summed up the significance of cyber risk for the enterprises thus: ***"There are only two types of organisations, one who have been hacked and others who don't know that they have been hacked."*** I observe that the schedule of the seminar is fairly comprehensive and I am sure that the participants would benefit from both – the presentations as well as from mutual deliberations and sharing of their unique experiences on the subject. In my address today, I intend to focus on two key dimensions of cyber security in banks: a) Internal Information Technology Security & b) Network vulnerabilities

Evolution of IT in Indian banks

2. I would begin by briefly tracing the evolution and adoption of Information Technology by banks in India. As regulator of the banking system in the country, Reserve Bank of India has played a very important role in technology adoption by banks. Rangarajan Committee on Mechanisation in Banks (1984) could be considered as the harbinger of adoption of technology for Indian banks. Thereafter, various committees / working groups have recommended gradual adoption of technology and need for associated safeguards in the sector. The journey of basically commenced with the advent of Ledger Posting Machines, moved to Total Branch Automation and then to Core Banking Solution (CBS). In the 1990s, the new generation private sector banks were mandated to commence their operations in fully computerised environment. As Gordon Moore's prediction of doubling of overall processing power of the computers every two years kept coming true, more and more applications in the banking space got pushed to the computerised environment.

3. RBI also played a very pivotal role in developing the payment market infrastructure and facilitating use of technology in the banking sector by setting up institutions like the IDRBT, NPCI, CCIL etc. Currently, these institutions provide the platform for running mission-critical and secured payment system applications like RTGS, Secured Financial Messaging System, Negotiated Dealing Settlement System etc.

4. Information Technology Act enacted in the year 2000 gave a further fillip to conducting of transactions in a computerised environment by providing a legal underpinning. Internet penetration gradually increased which led to increasing use of internet as a channel for delivery of banking products and services. The exponential growth of mobile phone users in the country also fast-tracked their usages as a delivery channel. The latest in the long line of innovations in the banking technology space is Unified Payment Interface (UPI), which has pushed the boundaries on remittances. To cut a long story short, technology adoption has increased manifold and today no bank can survive without robust technology, customer friendly digital products, hassle free user experience and continuous innovation.

Fintech revolution

5. With the advent of Fintech related innovations across the globe, well established banks are challenged once again. Today most of the banking needs can be managed through the mobile. Card based payments also have matured with the advent of pre-paid cards, tap and go, virtual card, multi-currency card, QR code based payments, etc. Technology has moved from being an enabler and differentiator to being an ultimate necessity and a way of life. By the end of this year, a handful of payment banks would have commenced their operations in India, stretching the banks on technology front. Some technological advancement that are gradually making a foray into financial sector include ***big data, artificial intelligence, block chain technology and internet of things***. Let me mention a few examples.

6. Banco Santander has expressed its intention to provide secure transactions using voice recognition via its banking app. RBS has trialled "Luvo", an AI customer service assistance to interact with staff and to potentially serve customers in near future. Japan's Softbank, in collaboration with Paris-based robotics experts, Aldebaran has developed Pepper, the world's first humanoid robot. Pepper is already being used in customer services industries as a replacement to an information booth or the welcome desk. Mizuho Financial Group Inc. bank has reportedly introduced Pepper to its flagship branch in Tokyo in 2015 to deal with customer enquiries, while Mitsubishi UFJ Financial Group has tested "Nao", a humanoid robot to interact with customers. Taking cue from their Japanese counterparts, I understand that HDFC Bank in India is also intending to introduce similar automation via robotics.

7. To buttress the point around increasing reliance on technology in the banking sector in India, let me reel out some statistics. As per the latest RBI Annual Report, the share of electronic transactions in total transactions in volume terms has moved up to 84.4 per cent from 74.6 per cent in the previous year. Likewise in value terms, their share has also inched up to 95.2 per cent from 94.6 per cent. At end-March 2016, the national electronic funds transfer (NEFT) facility was available through 130,013 branches of 172 banks, in addition to business correspondent (BC) outlets. NEFT handled 1.2 billion transactions valued at around Rs.83 trillion (approximately $ 1.3 tn) up from 928 million transactions for Rs.60 trillion (approximately $ 0.9 tn) in the previous year. In March 2016, NEFT processed the highest ever monthly volume of 129 million transactions. Similarly, the internet banking and mobile banking based payments are increasing at a rapid pace. I have already mentioned the UPI earlier. In this context, it will also be appropriate to mention the huge enrolments under Aadhaar (a unique identifier for residents in the country) with linkage to individual bank accounts, which in association with UPI has created an underlying potential to enable some kind of ***"account number portability"*** going forward. This can transform the banking sector in a way that cannot be fathomed now.

8. While everyone appreciates the ease of doing 24 X 7 banking transactions in a quick and efficient manner, the backbone for enabling such advanced technology based solutions is provided by the IT architecture of the banks. To optimally leverage new technology for providing new digital products, the IT systems at banks needs to be robust, capable of handling increasing volumes in a secure manner, providing connectivity to various applications accessing the bank's core banking solution in a safe manner and at the same time ensuring confidentiality of customer information. Recognising these challenges, Reserve Bank of India has been providing guidance to banks on managing the adoption of technology. Towards this end, one of the major initiatives of RBI was the setting up of Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (under Shri Gopalakrishna). The Group made important recommendations in nine broad areas viz. IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects. The guidelines, since issued by the RBI, clearly underlined that implementation of these recommendations needed to be risk based and commensurate

with the nature and scope of activities engaged into by individual banks as well as the level of dependence of the business processes on technology. Board level committees in the banks had been mandated to monitor the implementation of these guidelines in their respective banks. While substantial progress has been made in the past few years, I believe that banks still have to travel a lot of distance before the requirements are fully met. Given the centrality of technology in the functioning of banks today, this can no longer be treated as mere matter for compliance but has to be viewed as a core business issue.

Supervisory concerns

9. With computerisation of various activities within a bank, as a regulator and supervisor, we have come to expect much higher capability from banks in generation of relevant management information for decision making purposes. However, one feels that there is a substantial gap between the promise and the delivery. Let me highlight a few specific areas.

10. One of the primary areas of concern for the financial world is to ensure that the banking system is not abused by the unscrupulous elements for money laundering purposes. Regulations on Know Your Customer / Anti-Money Laundering are robust across jurisdictions. However, we often find banks not having robust systems to comply with the regulations. At the time of on-boarding of the customers, banks are required to assess their customers, their business and expected turnover in their account, source of such transactions etc. In recent times, we have come across several instances of banks having allowed transactions in their customers' accounts without any due consideration to their declared business profiles. The accounts received multiple RTGS/NEFT inward transactions and several such remittances were sent out of these accounts as well. Several accounts were abused to send money abroad in the form of advance import remittances. Despite the disproportionate activity in such accounts, the monitoring mechanism of banks fell short of our expectations. I wonder why banks are not able to devise fool proof ***technology-based solutions to identify such transgressions***. As you may be aware, RBI had to impose penalties on 13 banks for non-compliance with extant KYC/AML instructions including failure to categorise their customers in line with their risk profiles.

11. Another area that comes to my mind is the process for ***system-based identification of NPAs***. We feel there is much scope for improvement in this area. While we appreciate that the banks use multiple systems, the rules are elaborate and at times qualitative, posing challenges to capture the parameters in computer systems; however, with the progress in technology this problem should have been solved much earlier. What we expect is a robust system based identification of NPAs, not only for the regulator's use, but also for the banks' internal use so as to facilitate timely recovery / resolution.

12. The third area that I would like to touch upon is the Automated Data Flow project, wherein it was envisaged that banks would enable their systems for automatic flow of data for regulatory reporting purposes. I understand that ADF implementation has not progressed to the desired extent and despite significant progress on technology front, quality, consistency and timeliness of data submissions remains to be an issue.

13. I can go on. One common thread I see in all the above cases is the ***lack of Board level oversight and commitment from the executive management***. Technology service providers, particularly product vendors also have a role to play. It is important that the technology they provide is capable of meeting the regulatory requirements on a continuous basis and gaps, if any, are addressed within a short span of time and such upgrades flow seamlessly and in a cost effective manner to all of their clients.

Recent cyber incidents

14. Let me now turn towards some of the recent cyber incidents pertaining to the financial world.

- On 2 August 2016, Bitfinex, a Hong Kong exchange for the trading of digital currencies, announced that some of its customer accounts were hacked and bitcoins stolen. The value of the stolen bitcoins has been reported to be approximately US$65 million or more. As a consequence the value of bitcoins came down and the trust on the digital currency shaken.

- In the beginning of the year, Bangladesh Bank was the target and an attempt was made to steal US$1 billion and ultimately the attackers could successfully get away with US$81 million. Recently, in India too, a similar attempt was made on a commercial bank by generating fraudulent payment instructions on the Nostro accounts and transmitting them over SWIFT messaging system. Though monetary loss could be prevented with proactive follow-up with the concerned paying / intermediary banks, the incident has reinforced the fact that the various stakeholders have not learnt the lessons yet. We have also come across instances of fraudulent messages confirming documentary credits being transmitted using SWIFT infrastructure. Although, the latter incidents were mainly a result of failure of internal controls and non-adherence to "four eyes principles", it is also on account of reliance on disparate systems whereby SWIFT transactions could be done without originating a corresponding transaction in the CBS.

- In another incident involving shared mobile wallet of a bank, vulnerabilities were observed in the application itself which led to exploitation by the attackers. The originator of the transfer could get the amount reversed back to him without corresponding debit in the recipient's account in a large number of transactions (total amount involved was around Rs.12 crore). Bank was not performing any real time reconciliation and noticed it only when there was a spike in transactions which led to detection during reconciliation. The vulnerabilities exploited in the incident could have been averted, had the launch of the product not been rushed through.

- In another incident, an e-payment validation website of a large bank was hacked. Surprisingly, the bank was not aware of the incident till it was notified by a law enforcement agency. There was a Facebook post by a person from a neighbouring country claiming responsibility for the operation. Though the hacking incident did not result in any pecuniary loss as the site attacked was only performing validations of inputs entered by end users, nevertheless it demonstrates a serious security breach.

15. As may be seen from the examples quoted above, the cyber threat landscape is widening. This is natural, given that the money no longer moves only in physical form, but mostly through electronic means. It opens avenues for unscrupulous elements to devise ingenious methods for stealing it. One of the key targets by the attackers is the credential of the customers, as it provides the key to the "khazana (treasure)". Recent experience shows involvement of organised gangs and nation-state actors having huge financial backing. On the other hand, the cost of orchestrating such attacks is coming down. There are several reports indicating ***availability of credentials of customers for sale in dark web***, which is really scary.

Improving cyber resilience

16. Globally, the focus has now shifted to cyber security. Cyber security is no longer an isolated incident affecting one industry / one country. Several cyber-attacks in recent times have been designed to achieve political /religious objectives as also for securing funds for promoting terrorism. This has assumed frightening dimensions as it has an important bearing on financial stability. The importance accorded to the issue can be gauged from the fact that

global standard setting bodies as well as reputed central banks have been committing extremely large resources to address this menace.

17. Several countries have taken steps to improve their cyber resilience. Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (IOSCO) have issued Guidance on cyber resilience for financial market infrastructures in June 2016 after consultation with stakeholders. Financial Policy Committee (FPC) of the Bank of England launched the CBEST initiative – a Vulnerability Testing Framework. Following their meeting in June 2013, the FPC issued a recommendation requesting that Her Majesty's Treasury and the regulators work with the core of the UK financial system and its infrastructure to put in place a programme of work to improve and test resilience to cyber-attack. The committee also noted it was important that boards of financial firms and infrastructure providers recognised their responsibility for responding to those attacks. Recently, in May 2016, Hong Kong Monetary Authority launched a Cyber security Fortification Initiative(CFI). The CFI mainly comprises following three pillars:

(a) Cyber Resilience Assessment Framework;

(b) Professional Development Programme; and

(c) Cyber Intelligence Sharing Platform.

18. In India too, we have been working on strengthening the defence against cybercrimes. Government of India has taken several steps to tackle the menace of cyber-attacks and important institutional arrangements have been made. Indian Computer Emergence Response Team (CERT-In) has been established which monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the country. Banks / Financial Institutions have been identified as critical infrastructure for the purpose. A National Cyber Coordination Centre has also been established.

19. RBI has issued ***instructions on cyber security framework*** in banks on June 2, 2016. I am sure many of you would have had a chance to look at the instructions. Among others, the circular expects banks to put in place a board approved cyber-security policy, to prepare a cyber-crisis management plan, to make arrangement for continuous surveillance, to reckon the security aspects while procuring / connecting / implementing hardware, software, network devices etc., to ensure protection of consumer information, to share unusual cyber security incidents with RBI, to assess the gaps in cyber security preparedness on the basis of baseline requirements articulated in the circular and to set up a Cyber Security Operations Centre. The Reserve Bank also has set up an ***Expert Panel on IT Examination and Cyber Security*** (Chairperson: Smt. Meena Hemchandra) drawing representatives from the industry as members. The Panel is providing assistance in IT examination/cyber security initiatives of banks, review examination reports and suggest actionable items. RBI also launched a detailed IT examination programme in October 2015. This is proposed to be extended to more than 30 major banks during 2016–17 and to cover all banks by 2017–18. The Reserve Bank also proposes to set up a Cyber Security Lab, which will assist IT examiners in conducting analysis of cyber security of banks. RBI is also in the process of operationalizing its IT subsidiary (the Reserve Bank Information Technology (ReBIT) Pvt Ltd. The mandate for ReBIT, among others, is to focus on issues around IT systems and cyber security (including related research) of the financial sector and to also assist in the audit and assessment of the entities regulated by the Reserve Bank.

20. I am also pleased to note that IDRBT has released a comprehensive check-list on cyber security prepared by a panel of experts drawn from industry and academia in July 2016. I observe that the checklist covers wide-ranging aspects of cyber security like enterprise control, IT infrastructure security, Endpoint security, Security monitoring as also outsourcing security. I trust the banks/ financial institutions would find it very useful when

they try to benchmark the practices obtaining at their own institutions against the best practices indicated in the checklist.

Expectations from banks

21. Let me now share some of the expectations from banks. First and foremost, we expect the Board of Directors to get actively involved in the Technology related aspects. IT strategy needs to be closely aligned with the business strategy. With strides in technology, it would be difficult for Boards that do not have members having expertise in technology related areas to effectively adopt technology. ***Technology risk, including cyber-risk, is to be treated just like any other inherent risks faced by the banks viz. credit, market, operational risks*** and thus, Board needs to articulate what is their risk appetite, which residual risks they would like to carry and what kind of mitigation strategy they would like to follow. In the name of technology adoption, while banks are proactive in procuring various latest gadgets, what we observe across institutions is that the configurations of such devices are seldom given sufficient importance and left to the vendors. Vulnerabilities exist in hardware, middleware, software, OS, applications, network devices, communication devices etc. It is, therefore, important to pay sufficient attention while procuring / implementing any new devices/ solutions. ***Cyber criminals are also increasingly exploiting the vulnerabilities in the smart phone software by infecting the Operating systems with malware.*** The banks which are big on mobile banking as a service delivery tool must also look to guard against this emerging risk.

22. Another area of concern is the ***patch management***. OEMs release patches after known vulnerabilities are escalated to them and if the patches are not rolled out in time, we are practically leaving the door open for exploitation. User management leaves much to be desired-practice of shared passwords, no passwords, free administrator level access, dated authorized users list are quite common place. Often, there is no robust process for creating new users, reviewing the list and deleting inactive users. Then, there is the issue of implementing physical security. I have seen physical access control systems being in place but usage not insisted upon. Further, the dependence on the vendors is increasing and many a times only the vendors know how the system is to be operated. Customer information is stored at vendors' facility without adequate safeguards. Another curious thing I note is that while the banks claim that they do not get skilled resources, the same vendor provides some critical services to multiple banks. This raises a question as to whether the banks know what they get from their outsourced vendors, including the quality of delivery. Timely decision to scale up capacity is very important to ensure continued availability of services and business growth. People and processes need to be given adequate importance, for without capable hands even best of the systems is bound to fail. Monitoring is paramount – whether the port that was opened for a specific purpose was closed in time, who analyses the important logs that are created religiously, how incidents are responded to, whether the security operations centre (SOC) is integrated with inputs from various systems, whether the exceptions thrown out are escalated to appropriate levels etc.

23. ***The security culture at banks needs to change for the better.*** In a brick and mortar environment, if the safe is not having good locking system, or the walls are showing some cracks, roof is leaking, banks do notice. In a digital world, is it not important to look at such leaks, cracks and vulnerabilities and take appropriate action? Phishing attacks on customers are increasing. Is it not the responsibility of banks to educate their customers and build some work around to prevent the fraudsters to escape so easily? Considering the inability of the customers to withstand organised electronic crimes, ***RBI has put in a place a framework for limiting the liability of customers in unauthorised electronic banking transactions as a customer protection measure***. Similarly, whether it is technology service provider or SWIFT like infrastructure provider, is it not the vendor's responsibility to ensure that their agents meet all the electronic security requirements at all times and that the environment is secure enough to carry out the stated business? I feel society as a whole

need to recognise the emerging digital landscape and do their bit to ensure that our digital world, while it brings convenience and comfort to all the consumers, does not compromise the security.

Conclusion

24. In conclusion, I would like to recapitulate some of my observations.

- Cyber security has emerged as an important area of attention world over, particularly for the financial sector
- ***Cyber incidents are increasingly shifting towards targeting of financial institutions instead of end users.*** A manifestation of this trend is evident in Carbanak, a major advanced persistent threat (APT) attack against financial institutions around the world. The surprise factor in this APT attack was the criminals' change in approach and careful planning whereby rather than using the usual cybercriminal method of stealing consumer credentials or compromising individual online banking sessions with malware, the Carbanak gang targeted banks' internal systems and operations, resulting in a multichannel robbery that is estimated at $ 1 billion .
- Cyber risk cannot be brought down to zero. Hence a quick restoration plan with least damage post breach is crucial. ***There is a need to evolve a blueprint of co-ordination between financial institutions and public authorities in such an eventuality.***

25. The pace of expansion of digital world is increasing and hence, technology adoption should be conscious, purposeful and value adding. For improving the IT security, the banks need to focus on increased staff/customer awareness and training. Cautioning the staff and the customers to refrain from opening suspicious emails, emails from unknown persons, entering personal account details on fake websites, vishing etc. can be effective first steps in this endeavour.

26. While the financial sector has been ardently working for decades to prevent fraud and strengthen the detection and protection mechanisms, the threats to their internal operations networks has been considered to be low until attacks like Carbanak happened. Under the emerging circumstances, the banks need to be mindful of likely attacks from within the bank's internal core systems and try to plug such vulnerabilities. Banks need to practice "Cyber Hygiene" and I hope the Board and Top Management develop early sensitivity to this important task. The CISO also has a very important role in supporting the Board and Senior management in this initiative by focussing on IT governance, information security audits, customer communication, fraud management and legal aspects. Our view is that CISO's role needs to be enhanced from an operational level to strategic level.

27. I wish the Seminar all success and hope that the deliberations would be mutually beneficial to everyone and would help crystallise ways and means for a more secure, efficient and transparent banking sector going forward.

Thank you!