G Padmanabhan: Emerging issues in cyber security in the financial sector

Address by Mr G Padmanabhan, Executive Director of the Bank of India, at the Sri Chithira Thirunal Memorial Lecture Series, organised by the State Bank of Travancore, Thiruvananthapuram, 28 February 2015.

* * *

Assistance in the preparation of this address rendered by S/ Shri S Ganeshkumar, A Madhavan, Vaibhav Chaturvedi, Kashiap Balakrishnan, Smt Radha Somakumar and helpful comments from a number of colleagues is gratefully acknowledged. Errors, if any, are speaker's own.

1. It is not often that one gets an opportunity to deliver the very first lecture of a series organised in memory of a person whom you have known and respected from the childhood. One may have many things to say and eulogise about the Late Highness Sri Chithira Thirunal, but I can claim to represent a family which knew him personally and many of his family members. Therefore, I am thankful to Mr Jeevandas Narayan, Managing Director of State Bank of Travancore for starting this lecture series and giving me the unique opportunity of delivering the first lecture. It is also appropriate that the bank has started this lecture series considering the association of the Royal family with the setting up of this bank which has been well documented by Prof A Sreedhara Menon in his book, "Triumph and Tragedy in Travancore". The predecessor of today's State Bank of Travancore, Travancore Bank Ltd, started operations with a public issue of shares worth Rs 1 crore on October 8, 1945 which was oversubscribed by two and a half times the same day. The entire process was orchestrated by the government under Sri Chithira Thirunal and the inimitable C P Ramaswamy Iyer. Dr. Ludwik Aronson, a Polish Jew, whose expertise was reportedly utilised by the Reserve Bank of India for their Foreign Exchange transactions during 1943–45, was appointed as the first General Manager of the bank. The rest as they say is history and even today the bank continues to be the biggest influence in Kerala with the largest market share among banks and the mind-space among Keralites.

2. I chose the topic of cyber security, esoteric to many, as to my mind this area requires far more attention by the financial sector in India. Technology is quickly altering all elements related to end-to-end financial transactions. Infrastructures that support this transformation are increasingly becoming ubiquitous as they ought to be, more sophisticated and mobile. More importantly, financial transactions are increasingly getting processed in real time with lesser human intervention. End users are becoming more demanding for faster, more efficient, easier and more secure means of carrying out their transactions. At the same time, the financial sector is facing ever-escalating threats from cyber criminals. In an interconnected world, although all organisations are targets for cyber attacks, financial institutions are more vulnerable than most others. The vulnerability arises out of two reasons. One is the nature of banking. Banks deal with money. Money is today stored and transferred in digital form. An attack on banks can help the perpetrator to gain funds, which makes them the prime target. As banks have to keep their systems open to the customers unlike other vulnerable systems like defence, they are in general easier targets. So security in banks is not just important. It is essential. More importantly, the financial sector is based on trust. A customer would be willing to park his money with a bank if he believes that it is safe. In the digital world, the customer trust depends on the strength of security, or more precisely, perceived strength of security. This perception gets built on the experience of the customers. As more and more customers experience fraud – free transactions through digital channels, their trust in that bank is likely to be higher. Today, when the Indian financial sector is at a tipping point in technology adoption, when banks are going in for a revamp of CBS from being a mere transaction enabled system to a more modern information processing and

decision support system, the sector can ill afford to ignore the cyber threats that are getting increasingly sophisticated, systematic, and as some say even state sponsored.

IT security

3. Before getting into specifics of cyber security issues, let me talk about IT security in general. IT security implies that the IT systems including data are held in a secure manner and made available only to the legitimate users of the system. It implies protecting the IT systems, networks, programs and data bases, from damage, attack, or unauthorised access, so that resources are available for business transactions whenever required.

4. The security issues or failures can be broadly discussed under two segments- unintended and intended. The unintended failures largely occur due to IT systems hardware failure, application systems crashes, non-availability of infra resources such as power, bandwidth etc. All these factors could completely halt the business process with all-round negative fallouts. To address the unintended failures, an institution is expected to take several steps such as adoption of Board-approved IT governance policies, establishing data centres, third party contracts, robust service level agreements, IS audit etc. As far as the risk of unintended failure is concerned, the IT management policy framework that has evolved over a period of time along with corporate governance has addressed the risk factors to a large extent. All these have come at a huge cost, but a definite resilience has been achieved. However the intended intrusions to disrupt business, misuse the information available at the institutional level and to perpetrate fraud at the customer level continue to be orchestrated largely by a sophisticated group of cyber criminals.

Tackling cyber threats

5. While vulnerabilities in software and network continue to be the target of cyber attackers and defending these resources remain the focus of every organisation, the weakest link continues to be the user. Data breach arising from phishing attacks and social engineering continues to be on the rise. No doubt banks have made significant efforts to educate the user on safe banking, but it is often found to be inadequate in the face of a targeted attack. Social media provides the platform required for an attacker to mine information on an individual. This information is then used to make the user believe that he is communicating with a legitimate source. With easier access to social media and the tendency to share personal information, the number of users that are exposed to such attacks will continue to increase. Internet of things is no longer just a catch phrase. Today, a typical Indian home has mobile phones, tablets, laptops, smart TVs and gaming devices all connected to the Internet and with each other. It is estimated that by 2020 there would be 30 billion wireless devices connected to the Internet of things. Most of these devices have not been principally designed with security in mind. The issue that I am trying to flag is that as we acquire more and more modern electronic gadgets, there will be a large number of insecure devices that co-exist on the same network with more secure ones. Since in an inter-connected world, security is as good as the weakest link, the criminals will attempt to exploit a less secure but trusted device to attack the critical and well protected resources.

6. Mobile devices have been getting more powerful every year. Smart phones available today are capable of carrying out all the functionalities generally done on a PC. While there are efforts made to ensure that a PC is kept secure, a smart phone that does the same functionality does not receive similar attention. Mobile Banking has gained popularity in the last few years. In the coming years mobile devices are going to be increasingly used for transferring funds and for making payments. Mobile devices, if regular updating of security is given a go by, could well become an attractive and easy target for cyber criminals.

7. Large banks, retail establishments and restaurants are often the main targets of cyber attacks. In 2014, J.P. Morgan Chase & Co, the largest U.S. bank by assets conceded that unknown attackers stole about 76 million customers' contact information – including

names, email addresses, phone numbers and addresses. It also affected about seven million of J.P. Morgan's small-business customers. Mercifully, the hackers were reportedly unable to gather detailed information on accounts, such as account numbers, passwords, social security numbers or dates of birth. That these breaches happened even to banks like JPMorgan Chase that spend billions of dollars to fund IT budgets and employ large teams of security analysts points to sophistication of cyber attacks.

8. A survey conducted in the United States revealed that the cost of cyber crimes for the retail stores doubled between the years 2013 and 2014. Information of tens of millions of customers were stolen from retail stores Target, insurance company Anthem, formerly known as WellPoint, Anthem (ANTM) is the second-largest health insurer in the United States. In this context, FBI Director James Comey was quoted as stating "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."

9. The latest Kaspersky Labs Report-Financial Cyberthreats in 2014- highlights certain new, disturbing trends:

- Cybercriminals are becoming less interested in "mass" malicious attacks on users, preferring fewer, more "targeted" attacks.
- A shift in the cybercriminals' focus – instead of attacking end-users, they started to pursue organisations that work with financial information and payment tools.

The recent uncovering of estimated $1 billion heist against several banks is a pointer to the above. As per the report, $1 billion has been stolen in the attacks, which started in 2013 and are still ongoing. The gang, dubbed as Carbanak, used computer viruses to infect company networks with malware including video surveillance, enabling it to see and record everything that happened on staff's screens. In some cases it was then able to transfer money from the banks' accounts to their own, or even able to tell cash machines to dispense cash at a pre-determined time of the day.

10. Another concern is the increasing tendency of the insiders using the information they have about their organisation, against itself. Companies have no option but to trust their employees and provide them privileged access to systems. The Snowden incident in the US has clearly shown the amount of damage an insider can cause to an institution. It is easier for an insider to carry out a cyber-attack as he is already aware of all the security devices and procedures in place. An attack by an insider is often more difficult to identify and recover from. Attacks by nation states – cyber war – wars among nations are increasingly being fought in cyber space than on the battle field. Acts of cyber espionage are increasingly being reported and many nation states are suspected of being covertly involved. Cyber attackers that have the backing of the state have powerful systems and monetary resources at their disposal.

Need for robust policies and practices

11. As we have seen, any electronic system connected to a network can be potentially compromised. The best preventive solutions have been found inadequate to thwart a sophisticated, targeted attack by a motivated attacker. This is not to say that preventive solutions do not serve any purpose. Traditional prevention solutions like firewalls and Intrusion prevention systems help prevent a large number of known attacks and should be a part of any network, however, they are becoming quite inadequate as attacks become more sophisticated. For instance, a new but disturbing feature is the advent of malafide attacks on computer systems, which are difficult for even experts to identify. Some of the examples include malware which get attached to songs (which are commonly downloaded from recognised sites), or as links on e-mail messages. The malware gets itself installed in the computer of the user and starts watching the actions of the user. Some of the malware have the capability to read, recognise and record the commands and actions keyed in by

accessing the kernel (which is at the heart) of the computer and gather information such as user id and password of internet banking transactions. Once these are obtained, the information is transmitted to the hacker who could simply log on to the bank's site using safe (but compromised) credentials and siphon off money from an unsuspecting bank customer. By the time the customer realises this, the fraud is complete and most of the money is lost. There are reports that some versions of the malware "wear" disguises and have the capability of capturing the key strokes entered in the key board using the user's own camera on the computer! One approach towards ensuring that such attacks do not occur is to create a culture of selecting only those sites / addresses which we are very sure about as being safe and secure, which is commonly referred to as "white listing" of sites for granting access.

12. Today, tools like Security Incident and Event Management (SIEM), Network Behaviour Anomaly Detection (NBAD), Data Leakage Prevention (DLP), etc are available which provides deep visibility into operations and quickly detect a security breach. Besides, one approach being increasingly adopted by banks – apart from procuring tools and having rules – is following the age-old and time tested method of using analytics. We have all read about the advantages of Big Data and Big Data Analytics. While this is more often used for business development and customer behaviour analysis and customer preferences, there is scope of using this for mapping general customer behaviour patterns and whenever there is an exception or an outlier, the computer system could trigger a warning. For example, if a credit card holder has always been doing transactions in India, an SMS alert for confirmation could be sent when use of the card is noticed at let's say Malaysia. Or, if a computer user always browses data and speeches on the internet, when an attempt to download is performed, an alert seeking confirmation could be automatically generated. Thus, analysis of customer behaviour could result in pattern formation based on which exceptions could be highlighted by the computer itself, with little or no human intervention. This may of course necessitate some investment in the form of enhanced human resources with specialised skills. There are financial organisations in the world which have implemented these approaches with remarkable success.

13. What lessons do we draw from the foregoing? In this scenario, it is important to ensure that at the organisation level, the policy on cyber security clearly identifies different types of systems and data based on sensitiveness and criticality. It should set out the type of preventive measures required for each category, with critical systems having more stringent security. Cyber-attack is generally met with panic. A policy that clearly states the roles and responsibilities of each stake holder and the response that is required for each scenario will ensure that panic is replaced with decisive action.

International efforts

14. The biggest challenge in making the financial sector cyber resilient is to first acknowledge the complexities and interdependencies and then to proactively address failures, adopt effective resilience techniques, and resolve problems through cooperation. In order to cope with the idiosyncrasies of cyber attacks and enabling services to resume, the financial sector has to follow an integrated approach based on the adoption of a cyber resilience framework developed internally or adapted from a more generic framework – examples being: the NIST framework[1] (February 2014); the World Economic Forum's cyber resilience approach, (January 2014)[2]; and the MITRE framework (2013)[3]. However, it is equally important to recognise that any framework would not provide a one-size-fits-all approach to managing cyber security risk for the financial institutions.

---

1 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

2 http://reports.weforum.org/hyperconnected-world-2014/.

3 http://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14–0228.pdf.

Generally, cyber resilience frameworks aim to address three broad scenarios:

- Confidentiality breach, which involves confidential information being stolen.
- Availability breach, where the services provided are inaccessible or unusable upon demand by customers but where the systems per se are still intact.
- Integrity breach, which is the corruption of data or systems affecting the accuracy or completeness of the information and processing methods (and which could also impact the availability of services). The focus of the majority of cyber attacks continues to be on compromising confidentiality (eg stealing sensitive data) and degrading system availability (eg DDoS* attacks). An integrated approach has to address cyber threat holistically.

15. Let me highlight a few international initiatives in this regard that could be instructive. Bank for International Settlements through its Committee on Payments and Market Infrastructures has setup working groups and task forces to examine the issue of Cyber threats and have published reports on the subject to guide the industry in preparing polices to protect cyber resources. Based on these reports, I would like to flag a few key points that would need to be kept in mind while formulating a cyber security policy:

- Having multiple sites providing for effective recovery against traditional forms of risks however is mostly ineffective in recovering from a cyber attack. “Unintended consequence of resiliency” (for example corruption at the primary site gets replicated to the DR sites) makes them ineffective in case of a cyber attack.
- Systems at primary and DR sites are generally similar in architecture and equipment. This constitutes a major risk as the vulnerability that exists at one site is there at all. On the other hand heterogenic systems would be very difficult to manage.
- Periodic Real time, scenario based simulations is necessary to rehearse the management of a cyber security incident. The scenarios should focus on cyber attacks that could disrupt the normal day-to-day business functions, and the processes and procedures the incident response team utilise to address a cyber security incident.
- Business staff often spots a problem first, not the IT staff. Business staff is potentially best placed to see parameters changing dramatically and/or bottlenecks occurring where they shouldn’t. A process for business staff to quickly escalate such anomalies to IT staff will help in quick detection.
- Services of personnel with expertise in cyber forensics should be utilised to understand which systems have been compromised and to isolate them.
- “Buddy Banking” helps where operational management capability as well as the service itself is lost. “Buddy Banking” is where a second system or organisation is capable of taking over the functionalities of the affected organisation so that the service offered by the affected organisation continues to be available to its users. The usage of RTGS and NEFT as a backup to each other is an example in the Indian context.
- In case of a disaster, communication is the key. Robust communication channels with all stake holders should be available.

16. I would also like to draw your attention to two important initiatives undertaken by Bank of England towards ensuring cyber resiliency. The first relates to prevention and the second, recovery.

CBEST testing framework

17. Penetration testing services as they are currently conducted do not provide assurance against sophisticated attacks on critical assets. This is because testing is not done on critical assets because of the perceived associated risk and the testing is not done based on current and specific threats. Identifying this lacuna, Bank of England introduced CBEST. CBEST is a framework that brings together Cyber intelligence service providers, penetration testing companies and financial Institutions to deliver customised, intelligence-led cyber security tests in a controlled environment. The tests conducted by identified penetration testing companies replicate real world scenarios taking into account intelligence on cyber risks provided by the Cyber intelligence service providers. Further the tests are conducted on critical systems and essential services. This ensures that the critical infrastructures of financial institutions are tested with scenarios that are most relevant and which they are most likely to face in case of a real attack.

Use of SWIFT-MIRS as a disaster recovery system for RTGS

18. Unlike many other countries including India which maintain more than two sites for their RTGS system, the RTGS system in UK has two sites. BoE decided against investing in a fully operational third site as it was felt that the risk of losing both sites at once, though of critical impact, is very low probability. Further, in their perception, having a third site which replicates the technology platform of the first and second sites does not fully address all risks. A successful breach of one site would almost certainly lead to a breach of the second or third sites if they were exact duplicates. As an alternative, BoE considered the SWIFT MIRS initiative. The SWIFT Market Infrastructure Resilience Service (MIRS) is a generic RTGS platform developed and hosted by SWIFT. The generic RTGS system could be used by Bank of England (or any central bank) in the event that all their sites are lost. The Bank would continue to run the business operation, while SWIFT technically operates MIRS. Apart from offering an additional contingency option, MIRS increases operational resilience in two key ways. First, it will be technically operated from outside the United Kingdom, so bringing greater geographic diversity to the sites hosting the infrastructure. And second, MIRS achieves technical diversity as it will be based on a different technology platform. This addresses a problem common in contingency arrangements that sites share software and hardware configurations and so are susceptible to the same risks.

The way forward

19. The uncomfortable truth all of us need to come to terms with is that cyber crime is here to stay. Crime and money are often linked. Hence the financial sector remains most vulnerable in an inter-connected world. While what has been discussed thus far will be instructive to increase the defences and agility to deal with cyber criminals and attacks, I have a few suggestions as we look ahead.

Customer protection and legal framework

20. Today, a customer can use, apart from paper based instruments, debit cards, credit cards, automated teller machines, mobile phones, points of sale terminals or Internet for undertaking financial transactions. Cyber fraud can be perpetrated through any of the above medium/device. The Reserve Bank and the Government of India have been consistently making efforts over several years to encourage electronic banking and electronic financial transactions to bring the economy out of cash based system. If the efforts have to bring in sustained and substantial benefits, then the system has to be made robust enough for customers to have confidence in the system. For this to happen, the common person has to be safeguarded against any loss, as long as he has not been negligent, the onus of proving negligence being on the service provider.

21. In this regard, it is my considered view that India needs a statute protecting a common citizen against cyber fraud or cyber crime. A strong law, which protects a diligent customer from cyber frauds would infuse institutional safeguard to a common person and increase his confidence to use technology in financial transactions.

22. Let me quote two well known US based cases to support my suggestion. Take for instance, the widely referred case of Patco Construction Co., Inc. v. People's United Bank, 684 F.3d 197, (1st. Cir. July 3, 2012). The First Circuit Court of Appeals held the bank potentially liable for its corporate customer's losses after hackers intruded into the computer systems, stole the customer's bank account access security information, and used that information for effecting unauthorised funds transfers from the customer's account. In seven days, nearly $600,000 of fraudulent wire transfers were made from Patco's account by the time the fraud came to light. The Court found the bank's security procedures were not "commercially reasonable" under Article 4A of Uniform Commercial Code. Second, The Electronic Funds Transfers Act of the U.S. Federal Government and the Regulation E of the Electronic Funds Transfers adopted by the Board of the Federal Reserve serve well to protect the interest of the customer. The loss or liability for the customer is capped in case of card or the electronic transfers, if reported within a specific number of days and the limit varies depending upon the customer's compliance on the incidence reporting. This gives Federal protection against cyber crime.

23. One might argue that we already have RBI issued directives currently in place today to protect the customers' interest. Besides, institutions such as BCSBI, set up by the Reserve Bank has also been very active in setting up codes for protecting the customer interest. These are largely in the regulatory domain and the common person is not well aware of these nor are these seen as basic rights of the customers. The point that I am trying to flag is that a customer must be legally protected from suffering losses when he becomes a victim of the cyber crime as a matter of right rather than having to run from pillar to post to prove that he was not negligent. Today, for instance, if a debit card is fraudulently used causing loss to the customer, how long it takes for the customer to get the balance restored? I have come across instances -where even after fraud is proved- of banks waiting for insurance claim to be settled before the amount is restored to the customer. Is this fair? How is a customer concerned about the insurance arrangement that the bank has? This is where statutory protection helps. Can this protection also cover issues relating to cloud computing which could give a push for this cost effective technology being adopted more by the financial sector?

Customer protection and insurance

24. To implement the kind of customer protection as discussed above, it is important that the insurance sector also responds. Even in the US, the companies lament that the insurance cover does not give adequate financial indemnity to losses arising out of cyber attacks. What is the Indian position? The traditional insurance products cover risks against losses arising from natural calamity, theft, crime etc but typically do not cover losses arising on account of cyber crimes or cyber failures. An insurance cover against cyber crime or cyber failure would mitigate the risk to a large extent. There can be First Party as well as Third Party Insurance Cover against the cyber crime or failure. The First Party Insurance can cover losses faced directly by the insurance holder including personal information asset damage, including damage to the data, software, and a system failure due to cyber attack and post cyber attack crisis management expenses. The Third Party insurance can protect against claims for losses from another organisation or individuals affected by a cyber breach, including losses arising due to malware, virus etc. This can include network security liability, losses due to the theft and misuse of data, protecting against DOS attacks, liability costs due to internet publishing, including websites, e-mail, instant messaging, and chat rooms, crisis management expenses etc.

25. Insurance cover is certainly an option worth looking at as part of risk management, but this poses several challenges to both the regulator and the insurance companies. There are several issues in arriving at an acceptable formula for insurance premium due to paucity of historical data. We need to have systematic data on the losses suffered in the past due to cyber attacks covering incident occurrences and incidence reporting, impact analysis, third party damages suffered etc. This is certainly challenging but not insurmountable. I am confident that if we can find a way in arriving at a practical risk mitigating insurance solution, it would certainly add to the push of digital economy.

Cyber information analytics centre

26. Different institutions, different customers, individually or collectively undergo the pains of cyber crime. To my mind, we need to collect all the data, collate the attacks, failures, measures to mitigate the security gaps, the losses suffered, the turnaround time for fixing the security gap and analyse them in order to guide the industry participants as well as customers. This would also over a period of time, reflect the number of attacks, volume and value of loss, cost of correction and offer a wealth of information, apart from sharing the solutions for preventing known attacks. In particular, this effort would reduce the turnaround time for the sector as whole in bridging the security gap. IDRBT has started this effort last year. But a lot more needs to be shared to serve the full purpose of this important initiative. May I point out in this connection that when CIBIL was instituted to share credit and default status of the account holders, there was lack of enthusiasm from the banks in sharing information. But then, the regulator gave a push and today it has become a SOP (standard operating procedure) to check on CIBIL site. I would urge all the banks to proactively share information to IDRBT, which would help us to build a better response support system. We will not hesitate to walk the extra mile to make this happen.

Challenge is expertise

27. As we have seen, security is a function of four parameters – governance, policies, systems and awareness. Of these, the real challenge for the Indian financial system is the awareness. There are two kinds of awareness. One is the awareness among customers about the dos and donts in digital transactions. It may be required for banks to take upon continuous awareness campaign among all customers on the importance of information security and the abundant caution to be exercised by them. Internal awareness is the awareness among employees of the bank about security. While it is necessary to increase the overall awareness among all employees, it is imperative that a small section of employees are groomed to handle higher end security concerns, including digital forensics. Unless banks are able to have strong internal security teams, their position would be weak. Unlike other technology related activities, no organisation can afford to outsource its entire security. Banks have to take up measures to recruit and retain the right talent. More importantly, they should keep the security skills sets always alert and up to date in a world of constant threats by a more motivated group of skilled attackers. The challenge is that there is no readymade skill set in the market too. Banks have to build an entire banking security eco system themselves.

Conclusion

28. Let me summarise what I have been trying to communicate:

i) Cyber threat is real and is constantly evolving. No organisation is immune or can claim to be fully secure against a cyber attack.

ii) Preventive measures are a must in this scenario.

iii) Where prevention fails, make up with quick detection and decisive response.

iv) Every organisation should have an IT Governance Policy as a subset of cyber security policy. The policy should identify key assets, the risks they are exposed to, prescribe mitigation measures, roles and responsibilities in case of a cyber incident and state the response required.

v) Identify worst case scenarios and plan and practice the response in each case. This is challenging as one is facing a fast moving target.

vi) The aim should be to recover from a worst case scenario as set forth in the cyber security policy.

vii) Be an active participant in sharing information on cyber threats faced.

viii) Adopt ISO 27001 which is internationally recognised best-practice standard for information security management.

29. In conclusion, as Governor Raghuram Rajan warned in an internal communication, in today's interconnected world, eternal vigilance is the price we have to pay not merely for the benefits of democracy as the old saying goes, but also to enjoy the benefits of a safe and secure financial system.

30. Once again thank you for inviting me over and for your attention.