# Cyber Safe Financial Sector – A reality check and the way forward

Very good morning to all. Thanks for inviting me to speak at this Seminar where experts have gathered to discuss on the topical issues of cyber threat and use of blockchain technology. The organisers were kind enough to let me choose the topic, and I chose to speak on cyber security. There are reasons why I chose this topic. Policing the cyber systems is one of the toughest jobs. It continuously challenges the security personnel, administrators, regulators and the service providers. Whatever role you many play in this cyber drama, your task is onerous and daunting. As a die-hard central banker for more than three decades I was handling policies relating to safety of banks, their customers as well as securing the payment systems and the gateways from the intended attacks and unintended attacks and failures. Having crossed the sides, now a practicing commercial banker, I had to walk the talk by implementing the very policies, and provide advice and framework for ensuring safety and security on an ongoing

basis. I had about two years ago, while still a regulator exhaustively spoken about the topic at an event organised at Trivandrum. I thought i would use this opportunity to look at the issues from a practicing banker perspective .

2. There has been a paradigm shift of services and activities of the financial sector in the last two decades. The traditional brick and mortar boundary in most financial institutions is now the backbone of banking and finance whereas the technology provides the channels of servicing all needs of the customers. Thus, the cyber world and product innovation are survival tool kit.

3. Today, banks and Financial Institutions (FI) are using cyber as the media for almost all types of interactions, both financial and non-financial. While the banking transactions are front-ended with net banking, hand held devices and mobile applications, the non-financial transactions such as customer relationship management, delivery of various products and services, complaint redressal mechanism, providing product information, providing guidance to various stake holders, etc are also conducted through the

cyber facilities. The integration of financial services with the cyber world has resulted in enormous benefits to the financial sector as a whole and its customers in particular, to get service at the fingertip which used to take few days' time after multiple visits and facing long queues, not to speak of customer frustration. The productivity of banks and financial institutions have increased multi-fold after inclusion of cyber in their delivery channels.

4. Of late, there is a huge push from the Government for increasing coverage of the financial sector and moving away from cash based economy to an electronic transactions based cleaner economy. This is of great advantage to financial sector which can now extend its facilities to untapped rural India. This will be possible only through the cyber world by linking all villages and providing services using mobile devices at an affordable cost.

5. While the cyber world has facilitated a lot in enabling a new way of delivering services by improving productivity and reducing transaction cost, it has also resulted in various threats and challenges to ensure safety for wired

transactions. In the traditional brick and mortar model it was quite easy to provide physical security to those physical assets, as adversaries who were staying in the physical boundary of a country were well known and were less difficult to tackle. Whereas, it is quite challenging to understand and tackle adversaries in cyber world as it is boundary-less and extended to the whole physical world.

**Who and what are the threats in cyber world?**

6. As we all recognise, cyber-attack related incidents are increasing day by day and the attackers are very clever working as a team across countries with their vested interest. Every year millions of malware are injected in to the systems by the hackers. Symantec in its April-2016 report stated that, through its global network monitoring, it discovered over 430 million malware world-wide in 2015, up by 36% from the previous year. They are changing their methods, tools, strategy dynamically and it is becoming quite challenging to protect information assets. Wall Street Journal reported that even the web cams and digital video recorders are being hacked. This is very disturbing.

Security depends on CCTV cameras and the video recordings that are susceptible for hacking. Under such circumstances, ensuring safety of assets and information has become a continuous battle which can be won only through coordinated and collaborated efforts by all stakeholders. Let me now recapitulate a few recent financial sector related incidents:

**Hacking of ATM network:**

7. As you may be aware, there have been incidents where hackers penetrated the ATM network services provided by a major IT service provider during May-July 2016 and a few banks who had outsourced their ATM operations to this third-party service provider were affected. As per initial estimates, information of about 3.2 million debit card was suspected to have been compromised. Once the debit card information is compromised the entire amount in the accounts of the card holders is at risk.

8. How this took place even after implementing state of the art technologies with latest security tools is the pertinent question. The methods used by the hackers as per forensic

report is that hackers developed malware which is a piece of software code that could spread within the system of ATMs at an alarming rate. Using the malware they were able to capture the four digit PIN used for authentication during ATM transactions.

9. The question is how could a hacker develop such a malware? Whether they were aware of the detailed architecture of ATM solutions? How they could inject that source code to the ATM network? Does it also raise the issue that in an interconnected world we should be extremely wary of low end hardware supporting weaker formats that are vulnerable to compromise and hence adopt global standards? If we are able to answer a few of such questions probably we will be able to avoid similar incidents in the future.

**Bank of Bangladesh incidents**

10. That central banks were out of the radar of hackers was proved wrong when in February 2016, Bangladesh Bank, the central bank of Bangladesh, lost about US$73 million on account of malicious attacks. Central banks are making

huge payments using SWIFT platform. On this occasion, the payment instructions to steal money from Bangladesh Bank were issued via the SWIFT network by the hackers.

11. There were five transactions issued by hackers, worth $101 million where the payees were at Philippines and Sri Lanka. The event was brought to notice by central bank of Sri Lanka who observed that the transaction was not normal. They immediately contacted the Bank of Bangladesh who then discovered this heist. There were other transactions in the pipe line worth of million dollars which were stopped based on instructions issued by Bank of Bangladesh to Federal Reserve Bank NY.

12. The payments are done over a closed user network of SWIFT which has the best security technology solutions; then how this had happened? All the banking transactions are conducted through banking channels then why the amount could not be recovered? If answers to these questions are known, then solutions may also be easy to devise. It is now known that the hackers knew full details of the operation of the bank, the patterns of investment

messages, had access to the supervisory control modules and armed with all these, they could write malware which then resulted in the heist.

**Recent cyber-attacks on a private bank**

13. According to Kaspersky Lab, the well-known Moscow-headquartered cyber security firm had information pertaining to a bank in India which indicated that the security of the bank's computers had been breached. On investigation, this was found to be true.The modus operandi in this case was similar with a malware creeping into a bank's server. The malware reside as silent processes within the computer server system, they siphon off a whole lot of information which is then collected by the hackers. Such information can be used for blackmail or to inflict direct damage to customers. Most of the times the hackers are not within the boundary of our country, so it becomes legally difficult to take direct action against them.

**SWIFT Codes of some Indian banks Compromised**

14. In 2016, it was reported that some of the Indian banks' SWIFT codes were compromised. It was also reported that

since June 2016 at least 4 Indian banks were targeted but the hackers could not break in to transferring money. Not to take any further chance, banks are now comparing the documents that are received through SWFT with the documents deposited in the CBS of the bank.

**Recent Trends:**

15. A few recent surveys conducted by international agencies which interact with major global companies to collate information about the trends in cyber-attacks, modalities and suggest probable protective measures reveal the following trends:

- Phishing and luring users through various social medium and websites and organised call centres.
- A 13 per cent rise in phishing attacks was noticed in the year 2016, which indicates the increased activities of hackers in the cyber space.
- Injecting malware through various methods especially using advertisements, downloads and the like. Popular carriers of malware are browsers, Adobe

Flash etc. They are most oft used software and any un-updated version with a security leak would be a sitting duck.

- It was found that one-third of organizations that have been subjected to an attack lost 20 percent of revenue or more.
- The attacks were mostly on mobile devices, public cloud, cloud infrastructure and user behavior.
- Browser redirection malware is another type of attack, whereby browser infections expose users to malicious advertising (malvertising), which adversaries use to set up ransomware and other malware campaigns.
- The attack is now beyond size of business too. Small, medium and big are hacked without any partiality. What the hacker is looking in to the network is vulnerability.
- It is also known that more than 15% of incidents are not even detected, and therefore, till they are

detected, the hackers have free roaming time in the gullible network.

16. So, what can be done to take care and protect our most valuable information assets from malicious attacks?

17. I would like to use the analogy of medical science here to throw some light. A study done at leading hospitals reveal that about 30 per cent of the fatal cases in hospitals can be saved, if doctors wash their hands properly to avoid transmission of infections to already weak patients. In the same way, if we put in place proper information security policy and all the stake holders including customers follow some restrictive practices to avoid lucrative invitations on the cyber world, most of the attacks may be effectively countered.

**Challenge of Big-Data and cutting though the noise:**

18. Banks and financial institutions are implementing very sophisticated and costly tools as part of their information security solutions. These tools are generating huge number of audit records and alerts which are humanly impossible to monitor. Studies reveal that only 50 per cent of such audit logs are scrutinised. What does this mean? The tools available might provide alerts about incidents but nobody may notice them and therefore, no action is taken!

19. Another challenge pertains to the high frequency, high volume audit data (Big-Data) analysis using proper IT solutions. It is like searching for a needle in a haystack. Financial organisations need to build capability in this domain and ensure that audit logs are scrutinised regularly, as timely automated detection may save loss of information and malicious attacks and minimise cost of attacks, if any.

**Challenge of changing technology adaption, innovation and Group attacks:**

20. It is now evident that the Hackers' community is more united than others. Attacks are no longer isolated, but are

more synchronised and use collective innovation of technology for conducting targeted attacks. One of the recent incidents which was detected after lot of efforts is the File Less Attack. Attacks are also concentrated on special days/holidays.

21. Normally attacks are traceable and are identified by the existence of malware files in the disk space where they are saved for subsequent execution. In the case of file less attacks, the attack is done directly from the memory of the IT system. Even though they were considered file less, previous malware families would drop a small binary on the disk in the initial attack before moving into the main memory of the compromised host. However, the newest evasion techniques used by file less malware—Kovter, Powelike, and XswKit, for example—leave no trace on disk, thus making detection, which generally relies on static files on disk, more difficult. This type of attack was detected by analysing memory dumps where some irregularity was found in addition to the computer system behaving erratically.This is just one example how the hackers

community is continuously upgrading and building weapons posing challenges to the IT Systems and organisations as a whole.

**The Cloud Threat**

22. Cloud computing is catching the attention of many organisations. But do we have clarity about their threats? According to Netwirx Corp.'s second global Cloud Security Survey, it found that even though cloud service providers generally make security a top priority, cloud computing is still associated with a number of risks, including potential for unauthorised access by employees and third parties, sophisticated attacks, and lack of visibility into what is happening across cloud IT environments.

23. In addition, the old internal employee risk also exists in a big way in cloud based processing, In a study, it was found that the majority (61%) of respondents indicated that their own employees pose more risk to data security in the cloud than anyone else. And the overwhelming majority (95%) of respondents consider visibility into user activities in the cloud to be an important element in cloud providers'

security guarantees.The survey also found that the top three cloud security concerns in 2016 were unauthorised access (69%), malware (37%) and denial of service (DoS) attacks (34%)

24. Cloud security worries are accelerating as the technology goes mainstream: Security and privacy of data and systems in the cloud remains a top worry for 70% of IT professionals worldwide, up from 63% in 2015. And, loss of control over data is a worry for half of them (53%).

**Vendor / Third Party Connections:**

25. Many financial institutions have some linkages with third-party partners. Indeed, managing third-party risk is essential for financial institutions via established compliance measures, regular testing, frequent auditing, and limiting network access is a means to narrow the threat aperture. The concern is that there is a lot of dependency on service providers and there is a significant cyber security risk in that a lot of data is going back and forth and held by third parties. It is important that financial entities have robust vendor management systems and provide for their regular monitoring. To put it differently,

technology has ushered in new participants, making the eco system dramatically larger and more complex to secure. We are increasingly seeing non-traditional players entering payments/ banking transaction chain. As technology companies enhance their platforms by adding convenience of electronic payments, it needs to be recognised that data is being proliferated in more places through out the eco system. This is my view calls for, in addition to confidentiality and NDAs, global security standards featuring in vendor agreements.

**Mobile Threats:**

26. The first half of 2016 saw cybersecurity issues surrounding mobile devices, with Android devices receiving the bulk of the attention. Users need to be reminded of best practices: Downloading applications only from trusted vendors, realising that operating system updates may reset carefully configured privacy settings and ensuring that the mobile device has equal or better security than a stationary one since it is more portable and thus easier to lose or steal

– these are some of the facets to be understood by all users.

**How to make cyber safe financial sector?**

27. Although it will be presumptuous on my part to claim having understood all the granular technical details about the threats in the cyber world, let me nevertheless outline on what an individual organization can do and what the entire financial sector together can work to provide for a resilient and cyber safe financial sector. Ensuring a cyber safe financial sector cannot be an effort from an individual or a single organisation. It is a big stage, like a huge opera. Perfect coordination is called for to achieve a successful outcome. Let me try and amplify the role of various actors:

**The role of the Government:**

**28.** The Government policies, laws, institutional framework are of paramount importance. Where do we stand in this regard? The enactment of The Information Technology Act, 2000 together with Indian Penal Code having adequate provisions to deal with Cyber Crimes was the most important

initiative of the Govt of India. It provided punishment in the form of imprisonment ranging from two years to life imprisonment and fine / penalty depending on the type of Cyber Crime. Government has also set up cyber forensic training and investigation labs in most of the States. Although these are significant steps, the administration of justice system takes its own time.

## Financial Sector:

**29.** The concept of financial sector has undergone complete make over. Banks, financial institutions, non-banking financial institutions, primary dealers, stock exchanges and bourses, mutual funds, insurance institutions now form part of the financial sector. An attack in part of a sector can possibly have a domino effect. Since all markets are inter-related and integrated directly or indirectly, it becomes all the more imperative that coordinated efforts are made in defending the cyber systems in a holistic manner. An overarching cyber security implementation plan and immediate response action plan in case of deadly attacks need to be blue printed and established. With FSDC now in

place, there can be a regular and standarised agenda item on cyber security. This will also help in institutionalising the security system so that all regulators can act in a well-coordinated manner. The recently constituted inter-disciplinary committee at RBI is a right step in this direction.

**Importance of information:**

30. As I said earlier, we need to work as a team and establish proper processes to fight with the adversaries in the cyber world. This fight is quite different where you don't know much about the attackers and where they are from. Most valuable weapon is information itself.

31. We need to create centralised information warehouse on information security for Indian financial sector. The moment any critical alerts or any such suspicions are observed the same can be shared among all for health checkup. The first step is early detection to minimise impact as adversaries is trying to spread the malware very quietly. Sharing information will lead to lot of synergy of all the investments made on information security by the sector as a whole.

32. The information sharing platform may be build and maintained by a regulator like RBI or SEBI. The regulator is responsible for maintaining financial stability and hence may be required to play very critical role by creating organization setup for ensuring healthy financial sector IT infrastructure. Reserve Bank of India had already created ReBIT whose mandate includes ensuring IT security for the banking sector.

33. Next step should be creation of Incidence Response Team cutting across all areas of financial sector. The roles and responsibilities of the Team may include:

-Identification and categorisation of the event

-What immediate action to be taken at organisational level and at sector level to minimise the impact

-How to take care of press reporting

-What action to be taken in case hackers are blackmailing some entity as they got access to critical information

-Engagement of cyber security cell of Police and coordinating with Police by providing information

-Helping cyber police in investigation

**Regulatory Initiatives- Circular on Cyber Security:**

34. RBI has issued a quite comprehensive circular on Cyber Security on 2nd June 2016. The circular emphasises and clearly recognises that cyber security focus is distinct from a focus purely on information security.

35. The journey toward upgrading cyber security driven by this circular, though very exciting, is fraught with several challenges that banks have to address. Banks are already considering several cost reduction strategies to address cost pressures such as managing non-performing assets and shrinking margins. In the wake of this cyber security investment will not occur very easily. The circular highlights several aspects that banks need to adopt in their road map. However there is need to strike balance between a wish and realistic achievable objectives.

36. Banks should move from asset-centric security approach to establishing a holistic baseline security programme. Banks should guard against taking just a compliance-centric approach to the circular.

**Common regulatory authority:**

37. To avoid confusion and multiplicity of instructions all these should be covered under a single regulatory and supervisory authorities in a activity and service delivery based framework. The interest of the service consumers must be protected and a uniform digital identification and authentication framework should be worked out.

**ReBIT:**

38. Last year RBI set up a separate subsidiary called ReBIT with the specific intent of handholding the Indian Financial sector in its efforts to combat cyber security issues. It aims to proactively monitor the financial sector including undertaking ethical hacking of the critical market infrastructures to enhance the safety of the system. Besides, it is expected to assist the RBI during onsite audits of the data bases of the institutions and assure the integrity of the data bases and systems. This institution when it becomes full fledged is expected to fulfill the critical role of being the link and anchor in ushering in a cyber safe Indian financial sector.

**Financial Institutions – Roles and Responsibilities:**

39. Each and every bank and financial institution should treat cyber threat as one of the most critical threats of existence. The organization is required to make specific strategy and framework to manage cyber risk. This should include how to identify, manage and reduce cyber risk while providing state of the art cyber delivery channel for all innovative financial products and services. The role of a well prepared Information security policy has also been well entrenched. I presume that majority of members of financial sector had already implemented Information Security Management System (ISMS) or similar standards. Establishment of this type of system provides specific attention to Information Security need and continuous improvements keeping in pace with new threats that arise. The establishment, maintenance and continuous update of an ISMS provide a strong indication that an organisation is using a systematic approach for the identification, assessment and management of information security risks.

**The role of management**:

40. It is well known that it costs huge to maintain robust security systems. When the going is good, generally the expenses would be allowed to be incurred on the IT. But in lean periods, the management generally tries to cut corners by curtailing the expenses, especially the upgrades. There is a general feeling that if today the system is safe, then tomorrow it is bound to be safe and therefore there is no need to spend money on upgrades. We all know each upgrade, whether OS, RDBMS, security systems, all come with solutions for noted weakness and these patches address those vulnerabilities. Therefore, I would like to stress that when it comes to systems, let us not pull back the upgrades for budget sake. It could be counter-productive.

41. Analytics is the critical tool. We all know that humungous number of logs are churned out by various systems and subsystems. Minor incidents can go unnoticed in the heap of garbage and this can become full blown problem in future. Therefore, it is best to nip it in the bud. But for this, sound and sharp analytical tools need to be

deployed which would publish the results in the dashboard of the top management of the service providers as well as the customers. There are several products that are available in the market to facilitate this. The Machine Learning tools handle enormous amount of data, are intelligent enough, once properly parameterised, to pick minor/major incidents and report immediately. This would avoid occurrence of subsequent such incidents once action is taken. The advantage of such tools is that it would train itself of future incidents which otherwise could go unnoticed. But the attendant challenge is staff who can handle and interpret. Further, enlightened customers add enormous value. Customer education and empowerment has to be continuously pursued.

42. I feel there can be informal/formal coordination committees between institutions who use similar products so that they can take stock of the software suits that are deployed, the facilities and levels of security provided.This committee can also analyse incident reporting so that all minor and major incidents that occur in similar platforms are

known to all players and they can take coordinated remedial actions.

43. Even while deploying the upgrades, perhaps this committee can also work around the pricing factor, banking on the strength of the volume of orders

44. One of the critical issues the management should decisively act is on transparency. Whenever major incidents happen which affect the customer interest, I feel it is the duty of the top management to be transparent about the incident such as date and time of the incident, nature of incident, which type of customer could have been affected, what type of data could have been compromised, what remedial action was taken, what is the time lag between occurrence, detection and action taken. This suo-moto disclosure would go a long way in retaining credibility of the organisation as well as assuage the customer concerns.

**ICT Service Providers**

45**.** The financial world now cannot exist outside the technology orbit, be any of the activities. The service providers play the key roles in offering, implementing and

maintaining the technology services. It is well known that banks themselves have only a skeleton of staff highly trained in technology and they are more in managerial and decision making position rather than in running day to day affairs, direct monitoring etc. Their intervention is more through oversight, dashboards, critical incident reports and analysis thereof etc. Therefore, all financial institutions are excessively dependent on the service providers. India being the country which offers world-wide ICT services, ideally we should be the ones to be the beacon in addressing security concerns. But we look elsewhere for problem identification and solutions. Most of the MNCs who operate worldwide have presence in India, development as well as R&D. Should not these bigwigs take up independent research and offer bouquet of services to the financial industry in a coordinated manner. This need not be in conflict with competition and retaining the market share. Organsations need to think beyond the narrow confines of bettering the bottom lines of the balance sheet through the services done for financial sector. When state of the art solution is given at an affordable price, it would automatically show in the

balance sheet. I have, therefore, few suggestions for the service providers which includes OS, RDBMS, Networking, facility maintenance etc:

- ➢ Issue periodic updates to the top management of the customers the latest updates available, the latest fixes that plug the known vulnerabilities, the time and cost etc

- ➢ The management can place it to the Technical Committees for their recommendation to their Board for decision making process

- ➢ Instead of giving solutions in silos and always point to the complementary products for vulnerabilities, this exercise should be jointly done by all major service partners to address the issues in a holistic manner

- ➢ As soon as major incidents occur in one single customer site, alerts can be made to other customers who use similar products so that the abuse does not go viral across all platforms. This can be done maintaining confidentiality part. We have seen so

much of intensive and quantitative usage of technology by the customers as well as internal staff. Do the service providers take periodic surveys/studies on the software and facilities used by their clients, the ease of use, usage of security features, knowledge of security settings by the ed users etc? Would it not be of interest for them to know if the staff or customers do not use the safe guards because they are cumbersome or difficult or slows down the speed of the software etc so that these can be addressed in the upgrades.

**Conclusion**:

46. I would like conclude by mentioning that even if the cyber safe financial sector is kind of dream but it is possible to achieve the dream through coordinated efforts and continuous vigilant operations. In this context we need to concentrate on main five Pillars which are:

Institutional readiness (i.e. credit institutions, PSPs and financial market infrastructures)

Information sharing

Regulator – industry engagement (“social” dialogue)

Ecosystem resilience (e.g. identifying critical nodes)

Cross-authority and international collaboration (alignment of regulatory initiatives and actions)

47. I am sure that the deliberations of the day would centre around all these and I wish the seminar all success. Thank you.

**References**:

Cisco 2017 Annual Cybersecurity Report

Turnaround and transformation in cyber security India update – Pwc

2016 Data Breach Investigations Report 89% of breaches had a financial or espionage motive – Verizon

G7 Fundamental Elements Of Cyber Security For The Financial Sector

PPTs of ECB

Press Information Bureau, Government of India, Ministry of Women and Child Development, dated December 4, 2015