Cybersecurity challenges in the financial sector that is getting increasingly "wall less and roof less".

Dr Ramasastri, other members of IDRBT family, Participants at this prestigious seminar,

India can boast of many institutional firsts in the financial sector that became the toast of the world. CCIL, NPCI and IDRBT come to my mind readily. Each of them had played stellar roles. The earliest and the most important one among these was the IDRBT that with its unique mandate laid the foundation for digitisation of the financial sector in India by providing a safe and secure India network on par with international standards and continues to be the backbone infrastructure of the Indian financial sector. IDRBT had also developed messaging standards with digital signature capability even before SWIFT implemented digital signature. I have been fortunate to be associated with this institution in various roles-as a regulator, as a governing board member and as a member of the Rangarajan Committee that rewrote the role of this great institution.

Address by G Padmanabhan, Chairman, Bank of India at IDRBT on December 18, 2019.
The speaker acknowledges the assistance rendered by Mr A Madhavan, Mr K Ravikumar and Mr Naga Mohan Gollangi in the preparation of this address.

I am delighted to be back here and thank Dr Ramasastri for giving me this honour. Data or Information is power in an interconnected world and the financial sector is the biggest beneficiary of information technology and data. So, my comments would be prima facie related to the sector I understand the most and the one which is most vulnerable and most targeted as money is involved.

2. Most of you know I am a career central banker who has for last five years moved over to the receiving end from the proposing end. So, let me start by asking the question to myself, now that I am on the other side of equation having to vacate my mind of a central banker and in-doctrine that of a commercial banker, what in my view are the two focus areas of banks from the viewpoint of income or profits? I would say good quality credit portfolio and good quality technology adoption. To be balanced, let me also ask myself the question, what are the problem areas which could negate all the income or profits and put pressure on the bank balance sheet. My answer remains the same, bad loan book and poor technology implementation. The latter has big implication for the topic I plan to speak about- security of the financial sector in an inter connected world. Lest I am misunderstood, let me

state upfront my comments relate to an interconnected world and I am not pushing for common standards product-wise.

3. As we are aware, there has been a paradigm shift of services and activities of the financial sector in the last two decades. 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, handheld 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 stakeholders 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. 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 as well as wireless transactions. In the traditional brick and mortar model it was quite easy to provide 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. It is however a different ball game that is quite challenging to understand and tackle the unknown and unseen adversaries in the cyber world as it is boundary-less. The challenge of protecting open and faster delivery channels riding on blockchain coupled with 5G gets immense when "walls and roof" of banks are vanishing. At this stage, let me flag an issue that is unique to the Indian financial sector. In the Indian context, when 3-4 vendors have rolled out banking solution for the entire banking industry, if a security lapse is exploited by one rogue, then almost all banks using that solution become potentially vulnerable. It is as bad as cracking the password for one of my 5-6 email/applications when I use the same password for all accounts. This calls for closer cooperation or a common reporting authority and a common approach with the vendor.

Present Day National and Global Scenario

5. In the year 2018, cyber-attacks on India had increased by more than 100% over the previous year as against the corresponding global increase of 35%. India was the 2nd most targeted country for cyber-attacks in the world, after the US, which was in 1st place and followed by Canada in 3rd place, whereas India's global ranking in cybersecurity readiness stood at 47. India was ranked at 23rd place by UN out of 165 nations in terms of commitment of a nation to cybersecurity, where Singapore, USA and Malaysia topped the list in that order.

The changing landscape of cybersecurity

6. In one of the latest worldwide surveys, the confidence factor in cyber resilience measures has been found decreasing in the last two years (2017 to 2019). Bad actors have been seeking opportunities to take advantage of unsophisticated netizens or unprotected organisations since the dawn of the World Wide Web, but today's bad actors are in a class by themselves. Nation-state actors, often operating through a vast network of well-funded proxies, strive to exert influence, threaten stability, and sow discord through the mechanisms of cyberspace. Hacktivist organisations seek to

undermine, damage or discredit organisations whose agendas and politics they oppose.

7. **Certain recent Security Incidents**

- Malware found in most used CamScanner Android App with 100+ million users.
- Compromise of Twitter CEO's account.
- New SIM card flaw lets hijackers hijack any phone by sending an SMS (SIM Jacking).
- Cloud Security in question– Amazon Web Services (AWS) hit by DDoS attack bringing down the services for 8 hours-resulting in inaccessibility for many of its customers.
- WhatsApp hack by Pegasus malware to spy specific WhatsApp accounts in India during recent general elections.
- During the month of November 2019, 80,000 computers and 110 nursing homes across 45 states of US were attacked by Ransomware demanding a ransom of 14 million US dollars in Bitcoin.

8. After major incidents around the world in the past few years, many countries, such the United Kingdom, German,

Estonia, Australia, Canada and Singapore, have developed and issued laws to take action on cyber-security, such as the national strategy, guidelines of implementation and reporting. Generally, all cyber-security acts are focusing on industries identified as critical infrastructure (CI) or critical information infrastructure (CII) of the nations, such as national security, financial, telecommunication, public transportation and logistics, healthcare and energy sectors. These sectors are always the first primary target of cyber-attacks and cause the biggest business disruption or impact nationwide.

9. The latest Cisco security report flags the changing contours of cyber criminals. Cisco report flags three broad themes:

i. Adversaries are taking malware to unprecedented levels of sophistication and impact. For instance, the advent of network-based ransomware crypto-worms eliminates the need for the human element in launching ransomware campaigns. And always money is not the only concern but the obliteration of systems and data.

ii. Adversaries are becoming more adept at evasion—and weaponising cloud services and other technology

used for legitimate purposes. Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool, affording them more time to operate and inflict damage. Cybercriminals are also adopting channels that rely on legitimate Internet services like Google, Dropbox. This makes malware traffic almost impossible to identify.

iii. Adversaries are exploiting undefended gaps in security, many of which stem from the expanding Internet of Things (IoT) and use of cloud services.

10. **Some interesting statistics**:

- 91% of data breaches across the world happen by way of Phishing mails.
- 76 percent of cyber-attacks are financially motivated whereas majority of the rest are driven geopolitically.
- 67% of attacks were aided by significant errors of the victim.
- Over 80% of the breaches had patches available for more than 1 year, which were not applied.
- 75% of cases go undiscovered or uncontained for weeks or months.

- Smaller organisations, who are unable to spend substantially on cybersecurity, are targeted by the attackers (e.g., The recent case of a cooperative bank breach).
- Average time of detection after an organisation's network is breached – 220 days.
- Insider Threat – 70% - e.g., access of many sensitive files to all staff.
- 95% of data breaches are attributed to human error.

Challenge of Big-Data and cutting though the noise:

11. Financial institutions are implementing very sophisticated and costly tools as part of their information security solutions. These tools are generating a 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! 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 the loss of information and malicious attacks and minimise the cost of attacks, if any.

How to make cyber safe financial sector?

12. 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 we need to do and what the entire financial sector together can work to provide for a resilient and cyber safe financial sector. As I said earlier, ensuring a cyber safe financial sector cannot be an effort from an individual or a single organisation. Let me try and amplify the role of various actors:

Government Initiatives

13. 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 for 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. Some of the other steps include setting up of CERT-IN, National Critical Information Infrastructure Protection Centre (NCIIPC), National Cyber Coordination Centre (NCCC), and a dedicated Division under the Ministry of Home Affairs to deal with Cyber and Information Security. Although these are significant steps, the administration of justice system takes its own time. Perhaps, with the zeal with which the Govt is moving towards less cash society and pass all cash benefits directly in to the bank accounts, the next big step to be taken by the Govt is enabling infrastructure of fraud detection, arrest of the criminals and quick punishment.

Reserve Bank of India Initiatives

14. RBI has set up a Cybersecurity and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015. The Bank issued a comprehensive circular on Cybersecurity Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cybersecurity. In addition, RBI has mandated certain requirements on CISOs of banks and issued a circular requiring Board of Directors, CXOs and Senior Management of banks to be aware of cyber security and required them to undergo certification programmes. Recent monetary policy talks

about strengthening the IT environment of ATM Switch service providers. RBI monitors quarterly the status of each Bank with respect to this framework. The framework directs the banks to put in a place Board approved comprehensive Cyber-security Policy and effective surveillance covering network and data base security, protection of customer information , crisis management strategy. Supervisory reporting is another critical component of this framework. Security has to be top driven and hence the Board and Top management must understand the issues.

Establishment of ReBIT by RBI

15. Reserve Bank Information Technology Pvt Ltd (ReBIT) has been set up by the Reserve Bank of India (RBI), to take care of the IT requirements, including the cybersecurity needs of the Reserve Bank and its regulated entities. ReBIT focuses on IT and cybersecurity (including related research) of the financial sector and assist in IT systems audit and assessment of the RBI regulated entities; advise, implement and manage internal or system-wide IT projects (both the existing & the new) of the Reserve Bank as mutually decided between the Reserve Bank and ReBIT.

Role of Research and Academia

16. 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. I recall one of the incidents which was detected after a lot of efforts is the File Less Attack. This type of attack was detected after considerable efforts by analysing memory dumps where some irregularity was found in addition to the computer system behaving erratically. This is just one example of how the hackers community is continuously upgrading and building weapons posing challenges to the IT Systems and organisations as a whole. Countering this threat calls of dedicated and continuous research to monitoring evolving threats and counter measures. The financial sector depends heavily on academia for this. I would venture to suggest that financial sector should come together to fund such research on an ongoing basis. This would enable the institutions to be proactive rather than reactive in dealing with cyber-attacks.

17. Let me remind in this connection that security eco system for banks comprises government, regulators, banks, solution providers, fintechs, incubators and academic institutions. Fintechs have innovative tech as well as security solutions. As we are all aware, fintechs are getting support of

incubators set up by governments as well as academic institutions. Ideally the solutions emerge from academia which are delivered to banks through fintechs and IT companies. It is in this context that institutions like IDRBT which are at the intersection between industry and academia are playing an important role. Let me acknowledge in this connection, IDRBTs Centre of Excellence in Cybersecurity (CCS) that serves as the “one stop” resource centre for all Cybersecurity, Digital Forensics, tools, literature, and expertise for the banking sector. Apart from research, the Centre offers executive training programmes in various aspects of cybersecurity including Executive Education and Development. IDRBT further conducts cybersecurity drills every quarter, for the stake holders. Conferences like the present one will further facilitate excellent efforts of IDRBT in this regard.

Suggested Remedial Measures and Concluding Remarks:

18. Prevention is always better than cure. Methodologies suggested include threat hunting. It is an active security exercise, with the intent of finding and rooting out attackers that have penetrated your environment without raising the alarm. This is in contrast to traditional investigations and

responses that stem from alerts that appear after a potentially malicious activity has been detected. With all due respect to the role of latest sophisticated technologies, viz., Artificial Intelligence, Machine Learning, Block chain and even Quantum Computing in enhancing cybersecurity (these are also simultaneously a threat to cybersecurity), it is certain that no amount of sophistication would be effective unless the basics are strictly adhered to. What are they?

- Shift towards detection and response: - According to a recent study, average time the adversary stays and explores in the victim's network before actually conducting the attack is about 220 days. This has to come down. As it has been accepted across the globe that 100% prevention is next to impossible, timely detection and effective response would complement the gap to a considerable extent. There are tools available and RBI recommends automation of incident response.

- Back to the Basics - Basic cybersecurity controls can protect against the most common cyber-attacks, according to British government organisation the National Cyber Security Centre (NCSC). Not sticking to basics of security is the major threat in itself. This includes insecure configuration of systems and not applying security patches

on time leaving the known vulnerabilities open. For instance, a recent incident in an Indian cooperative bank could have been prevented had the security patches been installed on time which had been released a few weeks before the breach. Despite the attack being very sophisticated, the breach of network was too simple and could have been easily prevented had the basics been followed. Similarly, Microsoft released relevant patches weeks before the May 2017 Ransomware attack, but many had not installed the patches. Updating patches would have prevented a fair amount of people from being a victim. In this context, I would like to highlight the user responsibility too, be it customer, bank personnel or outsourced professionals. We are well aware that the hand devices, which have significant usage in banking transactions because they are convenient to use, are increasingly becoming severely vulnerable to malware. The malware infected devices could easily compromise security and bleed the customers/banks. We also read that the vulnerabilities that are found in the systems, be it IOS or Android, are being constantly updated. Are these updates carried out in user devices? If not, are these not injecting vulnerabilities to the banking network. What kind of precautions can banks take while onboarding the

customers onto digital platform? As a non-techie, I would not like to dwell on the remedies but I do want to provoke the researchers as to what best solutions can they come up with? Let me persist a bit more with this issue. We all know that while handling cheques and physical instruments, if the customer is found to be negligent in handling them, thereby compromising the security and validity of the transaction, the onus is put on the customer and not the bank. Similarly, if a customer is negligent, uses an insecure device, not updating, not downloading the app from the bank's own website, keys in all sensitive data in social media and unknown sites, why banks should be held responsible for the financial loss arising out of such losses? I strongly feel regulator need to come up with something on this front. Having said that, let me also argue in favour of the customer. It is becoming all the more difficult for the customers to differentiate the original from fraud channels, the duplicate mimic the original so well. But then the important downloads like the App should be downloaded only from the bank's website, and not from a public portal. I was just browsing through the apps of a popular private sector bank available in a public portal. There are more than 20-25 apps available for download. While scrutinizing, I found the review comments said these were not App but

taking to some webpage of the bank. Now this page can be genuine or a fake site. A gullible customer can end up downloading a wrong app and suffer damage with it. I hope the banks do have a surveillance mechanism to weed out apps that are masquerading in their name in public portals. This needs to be done 24*7. While all of us are keen that digitization should be way forward, definitely not with less responsible customers. This reminds us of a related issue to the apps of the banks. Banks are very security conscious and spend huge amount of money and efforts to beef up the security. They keep updating the hardware and software every now and then by following stringent process controls. Despite all these, to give feel safe factor to users and the regulators, I am of the view that a reputed institution like IDRBT should dissect such Apps and give a public certification of safety provided the basic conditions are met with by the users. Such a certification process would standardise the app scenario and instils confidence in users to adapt to technology. As far as cloud computing is concerned, it is perceived that the security issues are formidable as banking data is very sensitive and hence banks are hesitating to take to cloud computing though it could be cheaper. IDRBT should keep advising banking sector on this key issue and keep updating periodically. A

time would emerge when cloud computing issues would be addressed and safe to conduct banking operations from there, and at that point IDRBT can play a pro-active role in guiding the banks to migrate methodically, eschewing risks.

- Segmentation of Network – Segmentation of networks either physically wherever possible or virtually in all other cases will greatly limit the attacking capability of hackers even after occurrence of a breach.
- Regular Data backup is the best defense against Ransomware attacks: When a system is attacked by Ransomware we are left with only two options, one-to pay the ransom and get the system released from attack, which many a time would not happen even after paying the ransom. The second option is to format the system and re-install everything afresh. The operating system and even the application are re-installable but the data is unique. Having proper backup process will be the best defense against Ransomware.
- Awareness is the key: Continuous awareness campaigns for all stakeholders, viz., senior management, employees and customers. Once adequate awareness is in place, most of the things fall in place.

- Having a tight control over third party vendors: - Strong SLAs, regular audits, role-based access controls, multi-layer protection techniques and Database Access Monitoring tools will considerably reduce relevant risk.
- Implementation of multi-factor authentication wherever possible: This will powerfully address brute forcing and even many types of Phishing attacks.
- Effective usage of AI and machine learning-based tools: AI is certainly something of a double-edged sword when it comes to security. While solutions that utilise AI and machine learning can greatly reduce the amount of time needed for threat detection and incident response, the technology can also be used by cybercriminals to increase the efficiency, scalability and success-rate of attacks, drastically altering the threat landscape for companies in the years ahead. There is indeed an arms race playing out as you read this. Undoubtedly AI will prove to be boon to cybersecurity over the coming years – and it needs to be, because AI is also opening up whole new categories of attacks that organisations will have to be equipped to deal with very soon. I shall flag how Bots can be put to good use a little later.
- Automation of the on-boarding and security of IoT devices.

- Fine-tuning of SOC alerts to reduce noise: Going for Big Data based Next Generation SOCs is definitely good, however, it should be kept in mind configuring the SOC to reduce false positive alerts (noise) will play a great role making a SOC effective. Otherwise, the SOC's effectiveness will be compromised out of fatigue, no matter howsoever sophisticated the SOC is.
- Cyber Insurance: After taking all mitigating measures, to address the residual risk one should always go for adequate cyber insurance.

19. At this juncture , let me flag an issue that has been exercising my mind emerging out recent decision to merge some of the public sector banks. Mergers of banks is a complex involving several issues like culture. Among all tech integration is tough. That is the reason possibly banks chosen for merger are having same CBS solution. But the versions are different. Customisation is varied. Security solutions and controls in place are divergent. To bring together such systems over a period of 2 to 3 years retaining and rebuilding adequate security solutions and processes is tough. They can throw up security challenges. Banks have started these discussions. But they should focus on security

as much as on functionalities or user inter faces. The greater challenger will be skill set availability in security.

20. One of the less debated issues in this regard is the linkages with third-party partners. Even for a solo institution, managing third-party risk is essential via established compliance measures, regular testing, frequent auditing, and limiting network access as 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 cybersecurity risk in that a lot of data is going back and forth and held by third parties. Will a merger of different versions of CBS enhance the challenge? Another challenge relates to merging of SOC operations of merging banks. Different banks may have different set of controls and until these are fully merged the “weakest link” threat needs to carefully monitored and controlled.

21. Let me conclude by making a few remarks on (1) data protection and privacy issues and its possible impact on cyber/information security, (2) cloud computing and Bots. Data localisation is the buzz word around the world today. India probably has gone the distance that no country has so far. Will this impact the cost of security since we need to clone data centres in each country? Will it enhance challenges for network security ? In the scenario do we

redefine big data and advantages of centralisation? All these are emerging issues that the world has to grapple with. As far as cloud computing is concerned, it is perceived that the security issues are formidable as banking data is very sensitive and hence banks are hesitating to take to cloud computing though it could be cheaper. IDRBT should keep advising banking sector on this key issue and keep updating periodically. A time would emerge when cloud computing issues would be addressed and safe to conduct banking operations from there, and at that point IDRBT can play a pro-active role in guiding the banks to migrate methodically, eschewing risks. Finally, on to Bots. I would like to draw your attention on the usage of Bots, both in offence and defense of cybersecurity. Bad Bots such as Bot Virus, Bot DDOS, Bot Phisher, Bot Spyware etc., have been unleashed to attack the cyberworld with nefarious intentions. The attackers have improved significantly their efficiency as well made it more economical to indulge in penetrating the vulnerable installations and stealing information/data. As a result, the financial sector is one of the biggest victims. The Mirai botnet launched a devastating attack on large portions of the internet. Mind you, this was launched by youngsters, college grads. There was a worldwide network of infected machines which had a portion of their running

power diverted to launching DDOS attacks. Just as how the bad Bots are used, the defense must also emanate from a wide range of Bots. Defense Bots can become very efficient, proactive defenders, cheaper and capable of training themselves to adapt to changing variety of attacks. This alone can put the financial industry ahead on the defense curve. I feel IDRBT should play a pivotal role in unleashing security Bots to strengthen the Indian financial industry.

22. In conclusion, cyber security is a serious business today. Cyber security preparedness can often make or break an institution. Given the inter connected world and multiple payers this calls for a perfect symphony among the government and various regulators and other agencies. To me ensuring, a safe and robust 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. This is because the concept of the financial sector has undergone complete make over. Banks, financial institutions, payment system providers, non-banking financial institutions, primary dealers, stock exchanges and bourses, mutual funds, insurance institutions, all of them now form part of the financial sector.

An attack in part of a sector can possibly have a domino effect.

23. I am informed that what follows would be some very interesting presentations and discussion. Wishing you all a great seminar full of engaging, stimulating and fruitful deliberations.

Thank you[1]

[1] Address by G Padmanabhan, Chairman, Bank of India at IDRBT on December 18, 2019. The speaker acknowledges the assistance rendered by Mr A Madhavan, Mr K Ravikumar and Mr Naga Mohan Gollangi in the preparation of this address.