Key note address by Mr. G. Gopalakrishna

Banking on E-Security[1]

1. I am delighted to be amongst you in this seminar. While the group itself was officially named with a rather long phrase as 'Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds', I would like to add in a lighter vein that the organizers have done a rather good job of running a computerized optimization process and simply calling it as the "RBI's Gopalakrishna Working Group Report". At this juncture, as Chairman of the Group I would like to acknowledge the inputs received from experts in the Working Group who were drawn from various commercial banks, academic institutions, legal profession, professional bodies like IDRBT and DSCI apart from RBI. The Report has received widespread appreciation even internationally due to the depth and sweep of its coverage on IT related risks and the expectations it sets from commercial banks. As you know, the Guidelines were issued by RBI on April 29, 2011 based on Working Group recommendations after suitably incorporating suggestions received from all stakeholders. I would like to dwell in this Address on the origins of the Working Group, approach of the Working Group, broad overview of the Report, key issues that have been raised in respect of the Group's Report in my interactions with various stakeholders and critical points going forward.

Genesis of the Working Group

2. The Working Group was an outcome of a study conducted by Frauds Monitoring Cell of Department of Banking Supervision, RBI regarding frauds in various e-banking channels like ATM/debit cards and internet banking which revealed increasing trend. The potential for further increase in frauds was high given the combination of extensive leverage of technology at present and new types of cyber threats uncovered frequently in this cyber age. In this milieu, it was also important to maintain customer confidence

1 Key note address by G. Gopalakrishna, Executive Director, Reserve Bank of India at the Seminar on 'Banking on e-security – RBI's Gopalakrishna Working Group Report', organized by Cyber Society of India in association with Indian Overseas Bank at Chennai on January 27, 2012. Contribution of Shri N Suganandh, AGM in preparing the speech is acknowledged.

by furthering consumer protection measures. As a well known psychology truism goes "People don't react to reality; they react to their perceptions of reality." It is important to ensure that customers have sound perception of technology and security processes followed by banks. Also, there was no defined minimum level of regulatory prescriptions in IT. Some of the regulatory prescriptions relating to IT were quite outdated and a need was felt to update our guidelines. IT related legislations like the IT Act, 2000 and their amended versions needed to be factored into. It was felt that all the issues arising out of IT usage needed to be examined in a holistic and comprehensive manner. The outcome was an announcement of the formation of Working Group under my Chairmanship by the Governor in his Monetary Policy Statement in April 2010.

Approach of the Working Group

3. As per frauds related literature, there are basically three conditions present in a fraud - pressure or incentive, opportunity and rationalization/ justification for fraud. Among these three conditions, one of the important components to prevent or minimize fraud from a bank's point of view is the "opportunity" component which requires plugging of gaps or loopholes in control and assurance framework so that "opportunity" for perpetrating frauds is minimized to the extent possible. In case of e-banking, good IT governance processes, sound information security framework, and audit/assurance framework are important. Any weakness therein facilitate the frauds. Besides, areas like IT services outsourcing, customer education and IT-related legal issues need consideration.

4. Given the comprehensive remit of the Group, five Sub-Groups were created to cover the issues in the following focus areas: (i) Technology issues – Information Security and DR, (ii) IT Governance and IS Audit, (iii) Operational issues – IT Operations, BCP and Cyber Fraud, (iv) Legal issues, and (v) Customer Education. The objective was to draw from the global regulatory standards and best practices in relative areas so as to create minimum standards for commercial banks in India and to minimize differing interpretations among banks. We have also taken inputs from the AFI reports of commercial banks. The Group studied the existing circulars and guidelines of RBI as

also regulators in other countries, laws and regulations like IT Act, 2000 and IT (Amendment) Act, 2008, standards and reports issued by professional bodies, practices followed by banks and financial institutions across the world, and also discussed the practical issues with some banks, thereby gaining an understanding of the risks arising from emergence of new technologies, and benchmarked the requirements collated from various sources against extant RBI requirements.

Broad Overview of the Working Group Report

5. The Report has 265 key recommendations in various areas. These not only pertain to commercial banks, but also contain systemic perspective to enable the effective sharing of information and enhancing effectiveness of various measures for the banking industry as a whole. Crucial systemic recommendations relate to creation of multi-stakeholder forums in relevant areas and banker forums in various areas, facilitating sharing of best practices, cyber threat information sharing and alert mechanism, creation of an industry-wide crisis management set-up, need for declaration of banking sector as a critical infrastructure and provision of priority infrastructural support during exigencies. This is recognition of the fact that fighting cyber crime effectively is ultimately a function of the level of and cooperation among the relevant stakeholders.

6. I now present an outline on recommendations for commercial banks. The recommendations have two main dimensions. The first one pertains to the need for involvement of the Board and Senior level management (called as “tone at the top”) and providing for exclusive organizational governance structures in each of the areas. No major bank-wide initiatives can succeed unless the push and commitment comes from the Board of Directors and the top management. The second dimension relates to various policies, standards and procedures and implementing these effectively. These are indicated in the Report as “Critical Components of the Framework” in each Chapter. Through this systematic approach, the Group aimed to achieve a robust, consistent and focused framework of guidelines and standards in each of the areas under its consideration. The Group also attempted to maintain a balance between high level guidelines or principles based approach and detailed recommendations or rule-based

approach as per its judgement. Of course, achieving this is not easy given the complexity of the contemporary technology driven banking process – exemplified by the various layers of components and sub-components and their interactions, which together make up the information systems. The large size of the Report could be attributed to these factors coupled with the endeavour of the Group to holistically address IT related issues.

7. I now turn to other major recommendations of the Group which have also been indicated in the final RBI guidelines. The recommendations relating to IT Governance*, inter alia*, include IT Strategy Committee at Board level, IT Steering Committee, the need to establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistency between IT strategy and business focus, and IT project risk assessment processes for major projects. The largest Section of the Report pertains to information security so as to achieve robust processes to ensure confidentiality, integrity, and availability of data/information which is a key asset for the banks. From the governance point of view, key aspects of information security comprise the focus on the Chief Information Security Officer, reporting of information security function to risk management without having a direct reporting relationship with IT function, and the Information Security Steering Committee. One of the main expectations is the "defense in depth" approach where reasonable level of security is provided across various layers. International information security standard ISO 27001 is recommended for critical functions.

8. The Report has also highlighted the danger of compliance or checklist type of mindset and called for dynamic and proactive assessment of various threats and their mitigation. One of the important aspects is the focus on "information security awareness", as it is acknowledged that people often represent the weakest link in the security chain. In addition, the Report has called for enhancing the use of technology for identifying anomalous e-banking transactions, effective analysis of audit trails and logs, enhancing audit processes through the use of computer assisted audit tools, identifying vulnerabilities in systems and networks and using application systems for carrying out

critical business processes involving financial/regulatory/legal/MIS and customer related implications rather than through manual methods or through spreadsheets.

9. The Group has emphasized the importance of identifying the legal issues arising from use of Information Technology in the context of IT Act, 2000 and IT Amendment Act, 2008. Today privacy has become a key issue. The Risk Management Committee at the Board level needs to put in place processes to ensure that legal risks arising from cyber laws are identified and adequately addressed. It needs to be ensured that the concerned functions are adequately staffed and the personnel handling it are trained to carry out the function efficiently. The Operational Risk Group needs to incorporate legal risks as part of the operational risk framework and take steps to mitigate the risks assessed. The legal function within the bank should advise business groups on legal issues arising out of the use of Information Technology.

10. Report contains the recommendations to strengthen the business continuity framework in banks. I recall a funny quote from Garfinkel and Spafford “Those who do not archive the past are condemned to retype it!”. The need for robust backup, archival, DR processes and their proper testing apart from various other BCP and DR related measures have been recommended. The Report has a separate Chapter on customer education measures and the importance accorded thereto. As you know, leaving aside the big technology powered cyber frauds, many lateral thinking fraudsters seem to think that they need not waste time in mobilizing high-tech methods to commit cyber crimes when they could easily get confidential information by simply asking – I refer here to the “social engineering” techniques. It is important in this context, that customers are adequately and appropriately made aware of the various risks and protection measures in respect of e-banking.

11. Some of the recommendations are critical in context of compliance to Basel II and Basel III wherein IT systems need to have robust controls so as to provide assurance on the completeness and reliability of output generated by them. Further, as you may be aware, for calculation of capital, a new risk category “operational risks” has been added along with market risks and credit risks under Pillar I. Further, Pillar II of the Basel II guidelines

has required banks to devise an Internal Capital Adequacy Assessment Process (ICAAP) which is necessary to comprehensively consider all the risks faced by a bank based on its size, level of complexity, risk profile and scope of operations. Thus, while strategic and reputation risks are not part of operational risks as defined under Pillar I, these risks would need to be factored under Pillar II. The nature, coverage and underlying integrity of the ICAAP process are required to be assessed by banking supervisors under Pillar II. Thus, if various areas addressed in the Report are satisfactorily implemented based on risk assessment, it could provide confidence to the bank supervisor that the related risks have been minimized, leading to conservation of costly capital.

Working Group Report & RBI Guidelines: Issues

12. I now attempt to answer some key questions raised regarding the Working Group Report and RBI guidelines. It may be felt that implementation of such a large number of recommendations may be difficult for smaller banks. However, it should be kept in mind that the Group does not recommend a “one size fits all” solution. The implementation of the recommendations should be based on the nature and scope of activities engaged by banks and the technology environment prevalent in the banks. The RBI guidelines have also clearly stated so. Accordingly, we need to appreciate that today most of the commercial banks have core banking solutions and other critical application systems in various areas like treasury and risk management apart from various electronic delivery channels. Regulator expects a reasonable assurance from the smaller banks akin to larger banks and similarly a customer from a smaller bank should also not be disadvantaged in any way by banking with a smaller commercial bank. They should be re-assured that the smaller bank also follows minimum set of standards and good practices laid down by the regulator. Beyond the minimum level of requirements, various details have to be worked out by the individual banks based on a comprehensive risk assessment; and based on the outcome of such exercise, individual security measures can be tailored. Further, frauds tend to migrate to areas of least resistance (from secure to insecure banks) and hence their occurrence must be

prevented. We need to ensure robust technology related controls and processes at all commercial banks to facilitate customer confidence in our banking system.

13. Another comment is that the timeframe for implementation of guidelines appears to be aggressive. The final RBI guidelines had required implementation of basic organizational framework and put in place policies and procedures which do not require extensive budgetary support, and infrastructural or technology changes by October 31, 2011. Rest of the applicable guidelines were required to be implemented within a period of one year. The timelines is another indication of the seriousness placed by RBI on implementation of the relevant guidelines by commercial banks. RBI has also clearly laid down the broad approach which banks need to follow in implementing the guidelines. In order to provide focused project oriented approach towards implementation of guidelines, banks were required to conduct a formal gap analysis between their current status and stipulations as laid out in the circular and put in place a time-bound action plan to address the gap and comply with the guidelines. Given the fact that the guidelines are fundamentally expected to enhance safety, security and efficiency in banking processes leading to benefits for banks and their customers, the progress in implementation of the recommendations was required to be monitored by the top management on an ongoing basis and a review of the implementation status was required to be put up to the Board at quarterly intervals. Banks were also required to incorporate in their Annual Report from 2011-12 onwards the measures taken in respect of various subject areas indicated in the RBI guidelines. I also understand that IBA had formed various internal teams for implementation of the guidelines.

14. Another general question is whether RBI guidelines based on Working Group's recommendations subsumes earlier IT related guidelines. It has been clarified in the RBI circular that the Group had endeavored to generate self-contained and comprehensive guidelines resulting into reiteration of some guidelines already prescribed by RBI. However, crucial guidelines cannot be ignored as the nature of coverage is different. The relevant guidelines prescribed earlier would be an adjunct to the present guidelines.

15. It is also observed by a few that while the Report of the Group is largely technology neutral in respect of areas like two factor authentication for internet banking transactions, specific methodologies were suggested. Further, it is argued that some banks might have gone ahead and already made investments in implementing some specific technologies recently and it may be difficult for them to change quickly. In this context, I would like to state that the recommendations of the Group are broadly based on the best practices and guidelines issued by other regulators. One approach is that of the Federal Reserve who have indicated the various 2 FA methodologies/systems available and left it to the banks to implement the measures based on a proper risk assessment. The another approach is as followed by the Monetary Authority of Singapore which has specifically called for dynamic one time password based system or digital signature based system and have also recommended measures to address the man-in-middle attacks. While we have considered the best of the both approaches, we have leaned towards the approach followed by MAS, since the implementation of 2 FA and related measures were reportedly unsatisfactory in USA, as the banks chose the simpler and relatively insecure approaches. It should also be noted that presently in India, the banks face legal risk in not using PKI based digital signatures for authenticating electronic records, as indicated in RBI guidelines. Since few banks were found to be using poor authentication mechanism, the Group felt that banks should implement certain minimum level of standards relating to 2 FA authentication for critical internet banking transactions. Banks which have implemented other technologies may need to consider benchmarking the same against the regulatory and legal expectations and satisfy themselves about efficacy of the 2 FA methods implemented by them. In respect of security aspects, cost cannot be a limiting factor to provide reasonable level of security to enable customer confidence and protection of a bank's information assets. RBI guidelines had clarified that except where legally required, banks may consider any other equivalent/better and robust technology/methodology based on new developments after carrying out a diligent evaluation exercise.

16. Another query has been why ISO 27001 Standards have been advised to be implemented in certain areas which can have cost implications for banks. The ISO

27001 information security standards are prescribed only for critical functions such as data centre process so as to provide for a rigorous and disciplined approach to information security in such areas. However, there is no attempt to mandate the bank-wide process. It is felt that the recommendations of the Group on the relative areas are comprehensive. Other frameworks provided by reputed professional bodies like DSCI and IDRBT have also been recommended for consideration. Banks, as purveyors of public money, are always tightly regulated and the controls expected are of a higher order as compared to many other sectors of the economy.

The Road Ahead

17. At present, the crucial areas of concern are: Some banks still do not have comprehensive information security policies; the implementation is not effective; monitoring of SLAs in respect of outsourced vendors is not ensured; capacity management plans are not robust; appropriate vendor exit strategies are not in place; audit trail and log review processes are inadequate; IS Audit processes are not comprehensive; business impact analysis is not done professionally before drawing up BCP; there is lack of assessment of legal risk arising from IT related legislation; and the process of designing and development of awareness programs for customers is not in place. It is important to see tangible benefits to both customers and banks arising from effective implementation of guidelines by banks. The demand placed from all commercial banks is high and all commercial banks may have gaps, *albeit* at different levels, between their current state and expectations from RBI guidelines, which require to be bridged at the earliest. In other words, banks need to scale up the maturity levels in respect of all the areas suggested in the Working Group Report. Meanwhile, in September 2011 RBI issued guidelines on “Security Issues and Risk Mitigation Measures related to Card Present (CP) transactions” and indicated time-frames for their implementation. This is aimed at improving the security in respect of card present transactions.

18. I am sure you will acknowledge that the security is not a product but a process which requires all the sub-components to work together. As Edmund Burke stated long back

"Better be de*spised* for too anxious apprehensions, than ruined by too confident security." The key performance indicator is the quality and effectiveness of the measures taken and being proactive in managing and mitigating the risks. According to few comments heard, current degree of cyber crime and cyber frauds in India is not as bad as in western world and hence one need not be paranoid and focus too much on security and IT risk management processes. I would like to reiterate that a basic principle of information security is to be ahead of the curve and hence there is a need for robust and comprehensive measures. Further, we need to demonstrate effectively that we cannot let our doors open to cyber criminals, fraudsters and terrorists to break the faith of customers in our banking system. RBI is very sensitive to this issue and all the stakeholders need to ensure that we do not lose our guard during our journey ahead. The Working Group's Report can be considered to be a key deliverable in this context.

19. I am sure such seminars would certainly provide a forum for learning and sharing among the delegates who, I believe, would gain valuable incremental knowledge on information security by the time this event concludes. Together, we shall strive towards improving and sustaining secure banking processes and practices. I wish all of you the best in your endeavors in this direction. I wish the seminar a great success and congratulate the organizers for their efforts in organizing this seminar on such a key topical issue and for contributing, in their own way, towards the cause of transforming e-banking security in the Indian banking sector as also for enhancing the awareness of bank customers.

Thank You.