K C Chakrabarty: New paradigms in IT security in Indian banks

Inaugural address by Dr K C Chakrabarty, Deputy Governor of the Reserve Bank of India, at the Indian Bank' Association (IBA) – Data Security Council of India (DSCI) Conference on "Security Framework in Indian Banks", Mumbai, 26 April 2010.

Assistance provided by Shri G Padmanabhan, Shri S Ganesh Kumar, and Shri A Madhavan is gratefully acknowledged.

* * *

1. Shri M. V. Nair, Chairman, IBA and CMD, Union Bank of India, Shri B. Sambamurthy, Director, IDRBT, Shri Shyamal Ghosh, Chairman, DSCI, Dr. K. Ramakrishnan, CEO, IBA, distinguished speakers and panelists, IT and IT Security professionals, distinguished guests, ladies and gentlemen.

2. Information is at the heart of today's business, and the all-pervasive impact of Information Technology in harnessing, collating and processing huge volumes of information is definitive. In this scenario, the need for ensuring that information is kept confidential adhering to accepted norms of privacy and making it available to authorized users at the appropriate time assumes great significance. This is particularly valid for the banking sector where day-to-day operations are centered on information and information processing, which in turn is highly dependent on Technology. This conference on "Security Framework in Indian Banks" jointly organized by the Indian Banks' Association, the Data Security Council of India in collaboration with the Institute for Development and Research in Banking Technology as the Knowledge partner is thus not only appropriate but also of topical relevance to banks. This joint effort on the subject is extremely laudable and I deem it a privilege to be present amidst this distinguished gathering for sharing my thoughts on the theme of today's conference.

3. Banking as a business involves the management of risks based on a repository of trust extended by the customers. If this objective has to be accomplished, it becomes imperative for all security concerns especially customer sensitive data to be addressed in an effective way so as to ensure that the trust levels are well preserved and information assets perform the role that they are supposed to. While every banker understands the implications of financial risks, the risks arising out of the large scale implementation of technology and IT is not so well defined. Security in banks thus assumes significant proportions, comprising physical security in addition to the factors relating to security of Information and Information Systems, all of which have an impact on the reputational risk faced by banks.

4. Technology has augmented the scope, reach and coverage of banking through significant networking and the availability of a wide variety of new delivery channels to such an extent that the death of distances and death of identity has already been accomplished. In addition, banking is poised to be omnipresent through facilities such as "Anywhere and Anytime Banking", proliferation of services offered through ATM networks, IT enabled instant remittances across banks, customer payments, mobile payments and many more. The giant project of ICT supported Financial Inclusion is all set to change the face of Indian banking by making banking services fully inclusive.

5. Technology implementation has benefited the banks also due to the facilitation of the Reserve Bank – both from the operational and legal perspectives. In addition, the Reserve Bank had provided the broad framework for many innovative technology based systems. The guidelines on Internet Banking, and the Guidelines for Information Systems Security/Audit in 2001 were early initiatives aimed at ensuring safe and secure technology based operations by banks. Keeping pace with time and marshalling international practices, RBI has issued broad guidelines on mobile banking and prepaid (stored) value cards. These, along with the setting up of systemically important payment and settlement systems such as

Real Time Gross Settlement System (RTGS) and other retail payment systems like the Electronic Clearing Systems (Credit and Debit Clearing), the National Electronic Funds Transfer (NEFT) System, National Electronic Clearing System (NECS), Regional Electronic Clearing System (RECS), have transformed the way of banking and today's customers have a wide array of options to choose from. All these have safety and security at the heart of the respective systems.

6. A major area where IT security assumes significance pertains to the transmission of information using IT as a channel for communication. Traditionally, paper based systems have been subject to certain controls to ensure that the basic requirements pertaining to genuineness, authenticity, etc. are met with. These included verification of signatures, ensuring that there are no corrections, or if there are corrections, these are authenticated properly and so on. In the IT-based scenario, these aspects gain greater importance not only because of the speed with which IT based electronic information flows but also on account of the potential havoc that could arise on account of incorrect instructions.

7. The last decade witnessed a sea change in the way banking services are made available to customers. The implementation of Core Banking Systems has proven to be a big boon in providing anywhere access to banking services and the treatment of a customer as that of a bank and not as a constituent of a specific branch. With the interlinking of ATMs, the customer has been further transformed into constituent of the financial sector rather than a bank. Alongside, the banking sector has made significant efforts to identify security gaps in an IT enabled scenario and have addressed them effectively as well. The time is now appropriate to review the adequacy of the measures taken by banks. As the banks and IT industry came up with layers of protection for their systems, fraudsters, hackers and a bewildering variety of other such entities made voracious attempts at breaking the security layers. When the application layer was fortified, the attention was on to break the network layer. When the network equipment manufacturers hardwired the security protocol making it extremely difficult to break them, the attack switched over to the internet servers. Activities like phishing require customers and bankers to migrate to the higher levels of security. While these examples relate to Internet-based banking, the latest dimension relates to security for mobile banking. As the horizon of ICT keeps widening, the security gaps also keep rising, leaving the banks and customers lagging. It becomes essential that bankers, regulators, ICT manufacturers and system providers, software professionals and auditors all work in unison to proactively identify, anticipate and plug the gaps as a regular activity instead of acting after fraudulent attempts fructify. It is to be recognized that Information Security has two important dimensions, namely:

i. protection of investment in information assets and to the actual information thereon, and,

ii. availability of assets for use whenever and wherever required.

8. Management of fraud or attempted fraud throws open the challenge of response time in reacting which is very critical to avert further frauds and loss of valuable customer information. With advancement and globalization, cross border banking, cyber crimes from specific geographic zones would take deep roots if the cyber crimes are not responded in quick time. The entire industry would be benefited by swift action and system of reporting under a common umbrella, for which set standards specifying the action to be initiated at such times is clearly indicated. Though compliance to CERT (i.e Computer Emergency Response Team) requirements would address this issue to some extent, it would be preferable to have a dedicated institutional set-up for the financial sector to report security breaches, quick responding team for major breaches, monitoring compliance and reporting to the regulators. I believe that IDRBT can play a nodal role towards building such a set up. The major challenge would be to foresee the possibility of a fraud taking place and to have systems in place to avert them let alone responding to them after the event. It is necessary to address basic concerns relating to safety and security of Information and Communication

Technology (ICT) assets, to data and to information pertaining to the bank as a whole and the customer in particular.

9. Against this background, I thought that it would be appropriate to define a set of best practices which would enhance the value of IT security. I prefer to christen them as the "Ten Commandments of IT Security/Management in Banks". I shall dwell briefly on each of these now.

i. *Thou shall take adequate care of the human factor in IT implementation.* IT security is more often than not a people related aspect than a technical issue. This is applicable to both insiders and customers of banks as well. There is a need to be vigilant against an insider who may know more than what is required and when aided with unfettered access, could wreak havoc on the bank concerned. Equally important is a customer who exploits technology loop holes for malafide intentions. It is thus imperative that IT Security parameters provide adequate focus on the set of people directly related to the systems in addition to the targeted audience as well. In this connection, communication in a language understood by these stakeholders assumes critical importance.

ii. Thou *shall ensure permeation of IT security throughout the organization.* World over, it has been recognized and accepted that IT security is optimal if the implementation is top driven. The cue for this is that the Top Management of banks need to provide a missionary zeal for implementing IT security; their efforts would automatically ensure that the IT security related procedures are effectively implemented across all levels in the banks.

iii. Thou *shall have clear IT security policies and procedures.* One of the main characteristics of banking in India relates to the existence of well documented policies and procedures pertaining to their areas of operation. The IT security domain, however, cannot boast of a similar level of compliance. Well laid down processes and procedures not only enhance employee efficiency but also aid a great deal in ensuring that there is clarity of objective apart from acting as a veritable guide to the conduct of operations in a safe and secure manner. It is also imperative that these procedural requirements are fully disseminated to all sections of the staff for their unflinching compliance at all times.

iv. *Thou shall take action at the appropriate time.* It is almost impossible to achieve complete IT security in any organisation. Addressing IT security related concerns and breaches thus assume significance. The watch word here is timeliness; it is only those banks which take quick corrective action which can survive the onslaught of security breaches. Such prompt action is possible only if the banks have already put in place well defined systems and procedures. The need to focus on attempted security violations also needs to be taken care of since these offer themselves as excellent early warning signals which, if left unattended or improperly attended, may result in substantial losses and a small lapse often becomes a mega event due to lack of right decision at the right time.

v. *Thou shall ensure that adequate resource capability is provided for.* An effective IT security framework cannot be implemented in isolation. It is imperative that all resources which facilitate the accomplishment of this objective are adequately provided for. These include adequate personnel, effective and efficient IT systems, good vendor management policies, and sound IT/ARE Audit mechanisms. Costs are certainly associated with these but the benefits accruing on account of reduced impact of IT security breaches more than compensates for the costs incurred in this regard.

vi. *Thou shall provide for optimal Business Process Re-engineering.* Most IT implementations in the Indian Banking scenario are replicas of the manual work processes which have been only tweaked to perform in an IT-enabled environment.

The result is the existence of redundant processes and loss of efficiency. Business Process Re-engineering leads to cost savings, better work flows, improved efficiency and better customer service levels as Business Process systems are cross-functional, i.e. the system boundary is not within a single function but actually goes across boundary lines.

vii. *Thou shall take care of obsolescence issues for IT security as well.* Perhaps the only industry in today's world where advancements are very rapid and every advancement brings in its wake reduced costs for adoption is the ICT industry. Network based communication has reached rock-bottom levels as far as costs are concerned while the prices of IT systems have exponentially reduced. The rapid degree of product and feature obsolescence in the IT industry is a formidable challenge for banks. Such obsolescence needs to be tackled in a systematic and proactive manner for mutual benefit of the banks and their customers. Care needs to be, taken in such a way that upgradation to take care of technology obsolescence is performed in a scientific manner and on a need-to-upgrade basis. This would help banks avoid falling into the technology-obsolescence trap requiring huge sums of money for to come out.

viii. *Thou shall provide a framework for Incident Management.* Security related incidents cannot be wished away. The best tool towards an effective IT security framework would thus be one which acknowledges such security instances and provides for a framework for appropriate incident reporting within the organization and to the regulators. Such a mechanism would provide insights into the security violations and other such attempts, but the single largest beneficial factor would be the development of a set of knowledge workers who hold the key to success of any IT based initiative by banks in a country which can boast of some of the best IT companies runs by effective IT Czars.

ix. *Thou shall take care of Data Quality and Integrity.* The most vital component of IT security is the data which forms part of the IT enables business processing system. Data is hard to get or create, easy for misuse and is tough to be channeled towards beneficial interpretation resulting in meaningful analysis. To this end, banks need to work out effective standards aimed at high levels of data quality and integrity. I am reminded at this juncture of a book called "Database Nation" written by Simson Garfinkel which outlines the death of privacy in the twenty-first century. The author skillfully elucidates the various facets governing data piracy while concluding that the owner of one's own private information is not himself! Banks cannot afford to fall into this category and data refinement is one approach which would facilitate good data management with adequate levels of protective covers.

x. *Thou shall provide for IT security as a way of life.* The last commandment is more like a synopsis but is at the heart of all IT security related initiatives. IT security cannot be viewed in isolation; neither can it be implemented in fits and starts. Examples of good IT security implementation reveal that good IT security features are impregnated as essential requirements in a normal way of life. As banks, we need to imbibe the security culture in our normal day-to-day activities. This is a challenging and daunting task since the normal human mind is more attuned towards an easy, Laissez faire approach towards reduced security so as to enhance convenience. IT security does add on to inconvenience as it does towards increased costs, but it is economical in the long run.

10. Having set out the commandments; let me share a few thoughts of immediate operational relevance to banks. We have seen that the security standards has been evolving over the years and maturing along with the advancement of hardware and software applications. Financial sector has also been fine tuning and catching up with the global standards. All regulated entities have IT policy driven by their board and this policy has

various sub-policies such as Information Security Policy. The latest is the security standards for mobile banking. Banks have also put in place mechanism for IS Audits and these are seriously reviewed by the Audit Committee of the Board of the banks. While there have been conscious efforts on the part of the regulator as well as regulated entities, I still feel there is considerable scope in working towards having a uniformly accepted standards and practices for operational risks especially information security risks across all financial institutions. It is in this context that I have attempted to set out the standards for IT security. These are not intended to add on to the existing complexities facing banks in their normal operational levels; on the other hand, those banks which follow these would be well insulated against future shocks arising out IT security related outages. I am sure that in the world of today where only the fittest have any chances of survival, our banks will not only survive but also grow in prosperity and mature as well, using the best of Information and Communication Technology. The deliberations during the Conference would add value to the audience and I am sure that all of you would be more enlightened and be the better knowledge workers of tomorrow. It is this goal which we would have to achieve and to this end, I wish each and every one of you God speed and success. I am sure that the Conference would be thought stimulating, packed with high energy contents and be rewarding to you all. Let me conclude now by wishing the Conference all success.

Thank you.