V Leeladhar: Challenges in banking security

Inaugural speech by Mr V Leeladhar, Deputy Governor of the Reserve Bank of India, at the Banking Security Conference - 2005, arranged by the Indian Banks' Association, Mumbai, 22 June 2005.

* * *

Fellow Participants and Colleagues,

It gives me great pleasure to be in your midst, as we commence this workshop on Banking Security. I am particularly happy to be here to address a group of involved persons who are the harbingers of change - so to say - in the use of technology in Banking.

Banking as a business involves the management of risks. While much has been said about the financial risks, the risks arising out of the large scale implementation of technology is of recent origin, with banks having taken to large scale use of technology for their normal day-to-day business. Security in banks has thus assumed significant proportions, comprising both physical aspects in addition to those relating to Information, Information Systems and Information Technology, all of which have an impact on the reputational risk of a financial organisation.

In a world where geographical barriers are losing significance and the death of distances is already a reality, it is but essential that security be given prime importance in a transnational scenario where large sums of money are at stake. While the challenges related to physical security are those which can be confronted with relative ease, the position is much more complicated in respect of IT security. It is widely accepted that security is as effective as the weakest link in a chain. And, in the case of banking, the weakest link, in my view, does not relate to the components of technology (which do have an implication although), but on the person who is part of the information supply chain, and is typically the insider in the bank itself. This reminds me of an interesting or rather disturbing question one of the top police officials asked of the bankers in a security conference. "Are you keeping a track of some sort of the officials who left the organization ? Are you at least aware where they are now ?" There was complete silence around the table. He went on to clarify that most of the financial crimes had insider links. This is supported by studies carried out by international organisations. These studies have indicated that a substantial portion of the breach of security in financial institutions have occurred on account of, or have been triggered with the aid of internal exposures or internal controls being compromised. Against this backdrop, the security requirements of the banking sector need to be assigned high levels of priority.

Information Security is something which is best experienced than explained. All of us have at some point of time experienced the flow of information to persons others than to the intended users - even in a nonelectronic traditional environment. With networking and access to information being available at rates much larger than before, Information Security is an activity which provides some comfort to both the policy makers and the users of data.

The largest set of functions in the banking sector which has benefited from the advances in IT relate to payment systems since quick, safe and efficient transfer of funds across the length and breadth of the country is the requirement of the day. Security in Payment Systems cannot be addressed in isolation. It requires the integration of work processes, communication linkages and integrated delivery systems and should focus on stability, efficiency and risk control. Yet another prime aspect of concern in a good security policy is the role that the human beings have in a secure computerised environment.

It would be advisable to build security features at the application level in respect of banking oriented products, because of the critical nature of financial data transfer. The financial messages should have the under noted features:

- The receipt of the message at the intended destination
- The content of the message should be the same as the transmitted one
- The Sender of information should be able to verify its receipt by the recipient
- The Recipient of the message could verify that the sender is indeed the person
- Information in transit should not be observed, altered or extracted
- Any attempt to tamper with the data in transit will need to be revealed

- Non-repudiation

These features boil down essentially to **authentication** (to verify the identity of the sender of the message to the intended recipient to prevent spoofing or impersonation), **authorisation** (to control the access to specific resources for unauthorised persons), **confidentiality** (to maintain the secrecy of the content of transmission between the authorised parties), **integrity** (to ensure that no changes/errors are introduced in the messages during transmission) and **nonrepudiation** (to ensure that an entity cannot later deny the origin and receipt and contents of the communication).

I must add here that in a recent case of a co-operative bank, the entire operations, maintenance and management of the computer systems were totally in the hands of the firm which supplied the computer software and this led to a fraud and loss for the bank. Such cases cause reason for substantial concern. While the aspects relating to physical security leave a lot to be desired with even the most basic security requirements not being in place (like access for unauthorised personnel even to sensitive Cash holding areas), the security features in the computer systems are not fully fool proof in some banks.

There are at present a number of security standards available for different financial applications; most of them are internationally accepted and part of the ISO standards. These international standards should be examined and adopted keeping in view the requirements of the Indian banking industry.

Banks need to put in place measures which conform to there is policies and ensure the regular, periodical audit.

An important issue is relating to the security levels of use within the various operating departments in the banks. The common level of entry is the use of validation of authorised access (in the form of authorised User-Ids) to be further authenticated by correctness of passwords keyed in by the authorised users. Passwords often become 'passed' words in our context with no change at all in the passwords since passwords tend to be rather fixed for long periods of time. It is absolutely essential that passwords lapse after certain periods of time - generally not exceeding a month at the latest.

Authorisation of users is another activity that needs to be closely regulated and monitored. One of the basic requirements for implementation of security and monitoring thereof at the various departments is the need for system administrators. Most of our offices and departments have the system administration function clubbed to the normal operational functions assigned to a particular officer. The proliferation of networks within an office also acts as a negative factor in implementation of strict security features. Further, rights assigned need to be changed upon change of functions assigned to the operative staff and that updation, including those related to staff who retire have to be looked into.

There is an imperative need to imbibe a culture of security among all operative functionaries - whether officers or other staff and cutting across administrative gradings. Access to databases in computer systems and to the data contained therein have to be strictly restricted and not available to any but those authorised to make any changes in case of an eventuality for resolving a software lock / malfunction which is a conscious decision by the authorised personnel taken in conjunction with the head of the office concerned.

Change Management is another aspect that needs to be viewed from the security angle. Software (and at times hardware too), undergoes frequent updation and version control and levels of software in use across offices is an issue which needs to be examined in its totality for practicable implementation at all offices / departments.

I am sure that most of the newer software programmes would have all the essential and desirable features as mandatory part of their architecture. The software that are currently in use would have to be scrutinised from the point of view of conformity to the minimum security requirements that I had dwelt upon.

As leaders who would be using technology as a cutting edge towards excellence in services, you would all agree that these key requirements of security are required to be addressed in the sessions of today. It is gratifying to note the initiative taken by IBA in organizing such seminars and conferences which facilitate transfer of knowledge. I am sure that the deliberations of the day would be enriching to all the delegates.

I wish the Conference all success. Thank you.