Chapter 10. Road Ahead

In the process of investigation, researcher came across some findings not directly / proximately connected with the research on hand, or were compounded with other topics. In either case, these observations merit further and closer scrutiny that is not within the scope of the current research. Such cases are narrated here and planned to be taken up after the doctoral research is accomplished.
10.1 Further Segmentation

- Sectoral Segmentation – Current research has aimed at all the banks, however, the Indian subcontinent offers such a wide variety of banks that it would be really fitting to carry on this exercise – may be as a post-doctoral continuation – targeting the sectoral subsets as under

  - Public Sector Banks These banks have seen their growth span during 1970’s and 1980’s when the thrust was on spreading the branch network and serving the social cause. With all that legacy, they find it a bit hard to adopt the automation and penetrate it to far off branches in the areas facing infrastructure problems. Though these banks have been striving to keep pace with the global automation scenario, their limitations deserve a special study.

  - New Private Banks This class has been fortunate to begin their journey in 1990’s when
the IT was the in-thing and the social control on the banks was getting phased out. As a result, they are the silver-spoon banks with no legacy overheads and lots of freedom for computerization. They have naturally excelled using IT deployments and even used IT as a strategic tool as can be seen with ATM, Core banking solution, etc. These banks therefore are the forefront of technology usage and their IT security concerns are also of high magnitude.

- Old Private Banks

These are the banks in the middle strata as compared to the first two stated earlier. Being private banks they have liberty of choosing the technology, however, they have had certain constraints, too. These banks were not nationalized due to their relatively moderate size. In
some cases, it underlines their financial handicap in automation that is also to do with the conventional and conservative approach instilled with their organizational age and age-group of the average workforce.

- **Coop Banks** This category has come up from its roots still strong in the Indian cooperative movement. They are marked by their compact nature, localized scope, cooperation background, political interventions, dual control of RBI and Coop. Dept. Besides, of late this group has suffered considerable shakeout due to intrinsic financial weaknesses and the external factors like mergers and acquisitions.

- **Regional Rural Banks** These banks were formed with collaborative efforts of government
and commercial banks with a mission of serving rural populace with effective micro-finance. They have been a bit neglected lot on the automation front. Recently, some RRBs have taken some initiative, anyway, in the meanwhile the government has indicated a massive program of mergers of RRBs with the result there is a wait-n-watch strategy.

- IT sophistication: Technology deployment has shown quite a heterogeneous picture. At one end of the spectrum there are banks having all branches fully computerized and interconnected, several hundred / few thousand ATMs as well as Internet Banking. On the other hand there are still some banks where computers have just entered in past couple of years and are used as a simple tool without any high tech advantages of networks, etc.

It is therefore imperative that the research be taken ahead with specific IT background of the banks. Accordingly, there could be three classes of banks reckoned under High, Mid
and Low sophistication, with their distinct and special IT security needs.

- Size-wise Grouping   Lastly, the banks also need to be put in different slots as per their size. This could be on the dimensions of the business scale, branch network and workforce. This is necessary because researcher has faced certain problems to address a banks as differing in their size, as under
  - Assets – From below billion to thousand billion
  - Staff – From less than hundred to over one lakh
  - Branches – Merely single digit to five-digit count

10.2 Model Quantifications

- Models presented earlier has been devised after substantial brainstorming and thus has fifteen different parameters. While this is certainly a starting step towards reasoning out the training needs, there is still some scope for bringing about more objectivity. This could be done with rigorous quantification and that in turn means more elaborate study of those fifteen parameters to come up with a commonly acceptable yardstick for all. It also underlines the need and potential for automation in the process of training needs determination.
10.3 Model Application

- The model – after it is thoroughly quantified – could be taken up for real life implementation in some banks. Such an application of the model will vouch for the utility and also help reshaping / recalibration wherever needed to make it more and more polished. This task could not be performed as a control experiment and hence that is proposed to be taken up for the subsequent post-doctoral studies.

10.4 Vertical groups

- Some employee grouping is also envisaged, either as specialized officers or generalists at top brass level or at grass root levels, as under:
  - Specialist Officers
    - IT Officers
    - Inspection & Audit Officers
    - Security Officers
    - Law Officers
  - Generalists
    - Top Executives
    - Branch Managers
Need for addressing such groups has been underscored by the qualitative analysis as also by the quantitative analysis as stated earlier.

10.5 It would be an ultimate aim of this project to undertake the field study for some individual bank to figure out how practically this research could light the way of IT security mission of that bank.

10.6 Lastly, a sketch of an extrapolation mission is thought about. As earlier seen, banking has been a forerunner in IT deployment across all sectors and therefore the forerunner to sense the IT security problems, suffer and learn from security incidents and strengthen the IT security, too. This study could be well extrapolated to other walks of life heavily using IT like Telecom, Biotech, Retailing, Research Labs, etc. It is an humble yet resolute surmise of the researcher that this work could save some efforts and lead the IT security missions in the respective vertical segments.