Chapter 9.

Summary of Report, Findings and Conclusion

This chapter collates and consolidates the research findings to provide a gestalt of all the discerning in earlier chapters. It also presents the substantiation of the working hypothesis. Some clear pointers for the IT Security in Indian Banks are provided in the course as general recommendations and these would be a true contribution of research that would find certain application in the field in near future.
9.1 A brief summary of the major contents of the report is presented here as a quick single point reference to all the past chapters in this thesis.

9.1.1 Preamble is provided in chapter 1 to give a broad perspective of Indian Banking, its origin & history of different phases through which it has passed, e.g. social control, nationalization, mass orientation, later wave of privatization in nineties, etc. It also depicts the other streams of rural banking through RRB’s, etc. It then tracks the progress in terms of number of banks, the constitution of banks like public sector, private sector, cooperative and regional rural banks and also briefs on the size-wise categories of the banks. It tells about the branch network, population served per branch, business transacted per branch, followed by the initial efforts of automation starting from mid eighties till date. Finally the chapter offers a curtain raiser on the ever evolving IT scenario in Indian banks like Advanced Ledger Posting Machines (ALPM’s), Partial Branch Automation (PBA), Total Branch Automation (TBA), inter-connectivity among branches, Automated Teller Machines (ATMs) and Core Banking
Solution (CBS).

Main sections in this chapter are dimensions of diversity in Indian banking (section 1.1), major landmarks in the Indian banking as it evolved (section 1.2), key indicators on economic contribution (section 1.3), computerization phases (section 1.4 to 1.14), two major milestones in IT deployment at global scenario (section 1.15), regulatory initiatives for IT from RBI (section 1.17) and finally some reflections by the researcher in the remaining sections.

9.1.2 Chapter 2 on Research Background narrates how researcher started to have a feeling that IT security training in Indian banks needs certain improvements. It is during his corporate training and consulting assignments on IT security for many Indian banks, that he observed a sort of adhocism in the whole process and decided to treat this wide guess in a systematic manner using the structured and scientific research methods.

Before taking it up, the researcher also confirmed the hunch by consulting a few veteran bankers and IT executives in banks that they also shared the same apprehension that security training is minimal and the ignorance is aghast among the staffers.
Main sections in this chapter are the researcher's background (section 2.1), his interaction with and observations on banks (section 2.2), a kind of adhocism felt in IT security training (section 2.3), few glaring points of ignorance in the workforce (section 2.4), and other musings by the researcher in rest of the sections.

9.1.3 Chapter 3 on Problem Statement, Objectives & Hypothesis is drafted to formulate the problem statement and to set out the objectives that drove the research. The problem perceived was that the bankers at large have been obsessed with the IT as an enabling factor and they are not paying necessary attention to the flip side of the IT, i.e. IT security.

These objectives fulfilled twin purposes: Firstly, they helped to articulate the Hypothesis of this research. Secondly, they also provided some indicators to the research methods and the sample drawn from Indian banks. The objectives also helped to maintain the direction in which the research proceeded in the past few years and did not allow it to digress along side.

Main sections in this chapter are problem statement (section 3.1 & 3.2), research objective (section 3.3, 3.4 &
3.5), working hypothesis (section 3.6), research methods (section 3.7 to 3.10 and 3.22 to 3.26), population and sample (section 3.11 to 3.21).

9.1.4 Chapter 4 on Secondary / Literature Survey gives a detailed account of the umpteen sources traced during the research. This scanning and searching went in a cyclical manner, as one triggered other continually. The researcher has provided his train of thoughts that strings together these references in a coherent manner across the four broad sub-sections here, as under.

4.1 Indian Banking: This traces the fantastic progress the Indian banking has witnessed in the past few decades on any key factors like number and spread of branches, the deposits mobilized, advances deployed, the colossal workforce employed, etc.

4.2 IT Security: This section throws light on the IT security scenario on a very broad worldwide canvas and across several walks of life (mainly the banking and finance). IT also enlightens on the cyber crimes, the related techniques, scale of operations, innovative means, the victimized populace, the ruins they had to suffer, etc.

4.3 Training: In this part, the researcher has taken a stock
of the training in general and IT training in particular. It also dwells on the administrative problems in IT training as faced by Indian banks like deputing the branch people to far off training centers, the periodic transfers causing the bottlenecks in the knowledge management, ever-changing IT scenario necessitating the refreshing IT training etc.

4.4 Experience Survey: This is the first-hand experience of the researcher as collected across his umpteen IT security training programs he has conducted for many a banks constituting almost half the Indian banks. It talks of the modalities for training, the batch sizes, granularity of modules, the participation techniques he deployed, etc. The section also describes some path-breaking techniques used by the researcher, viz. the real life case studies / security snippets drawn from his training / consulting for cyber cell of police, etc. and also the suit of PC based games on the theme of IT security that he has developed and used successfully for numerous training programs.

9.1.5 Chapter 5 on Primary Data Collection speaks of primary data collection methods of questionnaire and structured / depth interviews. It then moves ahead with the quantitative
techniques of tables, factors, clusters, frequency
distribution, etc. that researcher has used to analyze this
data. Actual results of these analyses are provided in the
next chapter. This portion also classifies the survey
questions into various categories and narrates how the
survey was done not only by sending out the
questionnaires, but also hopping on to institutes of
national repute like NIBM, ASCI, NIA, etc. to get the
questionnaire filled up from a broad cross section of
bankers belonging to various rungs of organizational
ladders, from all regions, from all types of banks and from
all types of IT deployments.

9.1.6 Chapter 6 on Quantitative Analysis is in continuation of the
preceding chapter that dwelt upon the ‘how’ of the
analysis. What is presented here is the ‘What’ of the
analysis, i.e. the actual findings based on the quantitative
techniques, duly supported by numerous tables and also
correlation of certain observations that collectively try to
throw a new light on the topic. This is done by tabulating
the data not alone by frequency tables, but also clustering
it together to invoke some stunning results. It then moves
to few segmented compilations e.g. as grouped by internal
auditors, all IT Security professionals, Top executives, Faculty members, etc. working within the banking population.

Major section in this chapter are as follows: Section 6.2 provides a quick analytical look at the sample of the survey through seven tables, Section 6.3 presents approx. twenty-five tables for a simple / one factor analysis, Section 6.4 offers some multi-factor analyses by way of six tables, and finally a revealing section 6.5 on segmented queries that built up fourteen tables of responses from individual departments / functions within the banks.

9.1.7 Chapter 7 dwelling on Qualitative Analysis brings out some of the interesting observations the researcher made during the current exercise. These observations, due to their very nature, would transcend any efforts of merely quantification and tabulation. As the observations have a solid bearing on the IT security literacy among the Indian bankers, they are produced here with little ramification and interpretation by the researcher, wherever needed. Such observations are based on the depth interviews the researcher took and the necessary sources are also listed wherever applicable. This section is one of the real
findings that evolve during deft discussions with the senior thought leaders / opinion makers within the banking circles.

9.1.8 Chapter 8 deals with the IT Security Training Capability Model (IT STCM) devised by the researcher after contemplating all the past contents of research. The model aims to provide a mould that takes into account all the relevant inputs for IT Security training, attaches certain weights to these artifacts and transforms it into the training design. This mapping from paradigm to prescription should add value to the field. In all there have been fifteen causal factors identified and they are grouped under three heads. Similarly, a set of six training aspects that get impacted with the said fifteen causal factors is also identified. Furthermore, the interplay among these fifteen causes is also tracked. Finally, the six impacted factors also influence each other and that is also accounted for.

After this primary stage setting, the simulation process takes off which refines the results with each cycle to help the banks decide upon the training design for IT security. It is expected that this IT-STCM model would come handy to the banks which are otherwise going more by hunch or
adhocism.

Major sections in this chapter are Overview of the model (sections 8.1 to 8.4), fifteen causal factors in training and their multi-dimensional rubric (sections 8.5 to 8.11), Six impacted training aspects and influence of fifteen causal factors on these six aspects (sections 8.12 to 8.21), interplay within the group of fifteen causal factors (sections 8.22 to 8.23), interplay within the group of six training aspects (sections 8.24), final version of the model (sections 8.25 to 8.26), experimental implementation / pilot of the model (sections 8.27 to 8.31) and in the end the implementation guidelines for IT STCM model (sections 8.32 to 8.37).

9.2 After the above-said short recap of the report, next few sections provide the findings and then go on to prove the hypothesis.

9.3 It was found that IT security awareness is a burning issue already substantiated in the past chapters as indicated below with their specific references

- In the point 6.4 (i), it was shown that awareness of an Individual seems to be OK, but the organizational awareness if pretty low. This clearly means that there is a dire need for internalization / institutionalization of IT security.
Lots of Training on a continuous and en-mass manner would be the only answer. More about the modalities on training are provided in the next few sections.

- In the point 6.4 (ii), the awareness of the generic cyber crimes was found to be considerable while the banking specific cyber crimes was observed to be very low. As a step towards enhancing the appreciation of banking specific cyber crimes, an applied research, compilation and building up a sort of compendium is suggested, which could be widely circulated among one and all through house magazines.

- In the point 6.4 (iii), the need for the documented IT security procedures was established. Such need is felt for IT security policy, Business Continuity Plan (BCP) and similar topics. Banks would be benefited with undertaking an exercise of drafting and adopting the security policy and BCP and concentrate on the wide spread dissemination of the same.

- The point 6.4 (iv) talked of the need for more frequent revision of the IT security related documents. This is essential for keeping these documents current and agile. Banks should undertake more frequent review of said documents to keep abreast with changing technology and security solutions.
The point 6.4 (v) dwelt upon the security compliance to be boosted that is essential to send subtle signals to the staff that security is not merely a ritual, rather it is viewed seriously. The simple control like password has been loosely used by banking segment for almost two decades. Banks should increase the frequency and intensity of security reviews / security audits. Besides, they should start taking the unpleasant and bold steps to raise the sequel of disciplinary actions where the adherence is lacking.

9.4 Training is the single largest tool the banks can deploy to bring about desired change in the awareness of IT security. Following approaches have been suggested in the earlier chapters.

- Case studies This is an effective approach as it presents the real life cases to the participants and convinces them that such a thing has already happened and thus could happen to me / my bank, too. Equally, it tells the right way of mitigating the security exposures.

- Security snippets The lengthy nature of cases is a drawback in the fast paced life of today. Security snippets come handy as they are concise
and focus on one aspect of security.

Needless to say, that snippets are also drawn from real life incidents.

- **Extrapolation** These exercises help bankers to think hard and think of security threats in other walks, e.g. manufacturing, oil exploration, etc. This helps think from first principles, not to get blinded with stereo type security solutions.

- **PC Games** This is an innovative way with many merits, already detailed earlier. So here they are just enumerated.
  - Heavy concepts, Light encapsuled
  - Ease of play and yet latent learning
  - Longer retention of security doctrine
  - Sustained receptivity for 2-3 hours
  - No need of presence of the trainer

- **Train The Trainers (T3)** This has been particularly helpful in fast multiplication of the training programs, as the faculty members specifically trained in IT security training
could themselves conduct many more sessions in short durations

- Outreach Instead of trainees traveling from their place of posting to training center, the extension program would take the faculty to the place where participants are placed. This gives a tremendous boost to the effectiveness, cost and attendance of the programs.

9.5 The IT STCM model has been elaborated in the chapter 8. This iterative model could be utilized with increasing rigour by banks to bring about dramatic upward shift in the results of training on IT security. Initially the model may seem to be little bit lengthy for deployment, anyway, start up efforts will pay back substantially, as the bank goes ahead with iterative cycles of the model.

The model is definitely open-ended and the banks could add their flavour by add / change / delete of the fifteen causal factors of IT security training and / or six parameters of training, to fit their need. As of now, many banks are found to handle the IT security training in more or less adhoc manner. Such banks will certainly gain a direction to guide their efforts of IT security training.
9.6 An interesting research assertion is to bring about the desired change in the IT security mindset of one and all in the banks. Such a mindset change – absolutely essential as substantiated in the chapters 6 & 7 – could be taken up across various layers as under:

- **Top Management** – This layer is concerned with the strategic direction, sponsorship and the commitment for all the initiatives, including the IT security efforts. As of now, their awareness here at this level is low and thus not conducive to boost the IT security at lower rungs.

- **Middle Management** – This layer is responsible to monitor and control various organizational operations including IT security. To ensure an incessant security monitoring on their part, this layer needs to be provided with adequate training.

- **Junior Management** – This layer is currently trying to cope with IT security with meager organizational inputs and more on the individual security perceptions. To bring about positive change at this layer in implementing IT security at grass root level, training efforts could play a solid role as stated earlier.

9.7 While some of the past chapters accord a qualitative endorsement marking the accomplishment of the research mission, the working hypothesis of this research is substantiated in next few sections.
9.8 A list of top ten important questions was drawn from the survey queries put to various bankers & IT professionals. The selection of the questions was confirmed with the miniscule opinion poll of the experts in the field. These senior & veteran officials in the area of IT security in banking have seconded the choice of following ten survey questions as the most significant. These questions along with the percentage score of the ideal / expected answers during the survey are enumerated below

<table>
<thead>
<tr>
<th>Top Ten Significant Questions in the Research Survey</th>
<th>% Score of Ideal Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is IT security policy circulated across all employees?</td>
<td>45</td>
</tr>
<tr>
<td>2. Are there any procedures on logical access controls?</td>
<td>43</td>
</tr>
<tr>
<td>3. Is the concept of Data ownership documented?</td>
<td>43</td>
</tr>
<tr>
<td>4. Are there any procedures issues on Email?</td>
<td>44</td>
</tr>
<tr>
<td>5. Is any safeguard taken for Laptops carried outside?</td>
<td>5</td>
</tr>
<tr>
<td>6. Do you know Salami technique of cyber-crime?</td>
<td>38</td>
</tr>
<tr>
<td>7. Do you know what is trap doors / back doors?</td>
<td>7</td>
</tr>
<tr>
<td>8. Do you know significance of Denial of Service Attack?</td>
<td>34</td>
</tr>
<tr>
<td>9. Have you received, read &amp; understood Bank’s BCP?</td>
<td>25</td>
</tr>
<tr>
<td>10. Are there any trials to test the BCP effectiveness?</td>
<td>18</td>
</tr>
</tbody>
</table>

Average Score for above responses 31

Table 20 : Top 10 Significant Questions in the Research Survey
9.9 Some interesting observations here:

- The questions are selected from the questionnaire based on the criterion of ‘organizational preparedness for IT security’.
- The selection of questions is backed by IT security experts with extensive experience in the area.
- These questions point to the training initiatives to be taken by the banks for enlightenment of the workforce. Employees cannot be expected to take such steps on their own.

9.10 None of the above-said ten questions got 50% assertion, while the overall or averaged score is a meager 31% that unequivocally attests the hypothesis in a quantified and objective way.

9.11 In addition to above, following recommendations are made that are based on the generic IT Security experience of the researcher (research in broader sense, not specifically confined to survey)

- IT Security training should be given its due status, as it has got potential to avert many undesired security incidents.
- Opportunity cost of such training is very high and this point needs to be imbibed among the top rung of the banks.
- It then follows as a corollary that IT security training should be viewed in the same way any nation treats its defence.
• As technological advances in the field of IT are very fast, the need for related training should be reviewed incessantly.

• There should be commitment from the senior management and better skills at middle tiers on operational IT security.

• Change champions would be effective catalysts to bring about security hardening, that is otherwise a low priority.

• Cultivating a security mindset would be of immense help to the bank staff in striving ahead on security continuum.