Chapter 8.

Model Proposed for IT Security Training

This chapter narrates IT Security Training Capability Model (IT STCM) devised by the researcher. The model aims to provide a mould that takes into account all the factors relevant 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.
8.1 As earlier seen, Indian banking segment exhibits quite a diversity when it comes to IT drivers and business parameters of various nature. It is a full spectrum of umpteen banks that are heterogeneous on multiple dimensions like constitution, business scale, branch network, IT deployment in terms of sophistication and spread, etc.

8.2 It is therefore a formidable task to arrive at a common denominator for such a rich variety. Still, IT Security Training Capability Model (IT STCM) model is attempted here that takes into consideration

- 15 Major contributory factors (causes) that influence the IT security training in various ways explained hereunder
- 6 Key impacted factors (effects) of IT security training that are influenced by above said fifteen causes
- Interplay of the Causes among themselves, i.e. some causal factors influence other causal factors
- Interplay of the Effects among themselves, i.e. some effects have a ripple impact on some other effect factors

Due to this, the IT STCM has grown into its complexity and number of parameters it tackles.
8.3 To smoothen the process and to help handle manageable chunks at a time, an iterative use of model is suggested as elaborated below.

8.4 Pictorial view – that is also essentially unfurled in four versions – of IT STCM would help conceive it better. Here is first version:

![IT Security Training Capability Model (IT STCM) – Version 1](image)

Figure 53

8.5 Coming to the fifteen influencing factors (causes) of the IT security training The model basically reckons a set of three influential broad groups, viz.

- Human Dynamics
- Business Paradigm
- Tech Deployment
8.6 Each set has certain potential to impact the IT security training and to ascertain it in its entirety and subtlety, these sets are further exploded into the individual factors influencing the IT Security training, as under:

8.6.1 Human Dynamics

- Total Workforce
  It talks of the employee count of the bank across its complete network of branches and across all rungs of ladders.

- Technical Awareness
  This factor reflects the overall awareness of the workforce about IT in general and IT security in particular.

- Work Quantum / Load
  It gives an idea about the work load per head in terms of an average amount and transactions tackled by each staff per day.

- Cyber Crime Techniques
  Current trend of cyber crime (exploit by an outside human factor of hackers) is denoted here as techniques, spread & rate.
- Staff Turnover

  It throws light on the ever changing pattern of branch team of the bank due to transfers, retirements, resignations, etc.

8.6.2 Business Paradigm

- Branch Spread / Network

  It quantifies the branches of the Bank penetrating various parts of the geographical area of India.

- Business Volume

  This parameter shows the business (i.e. accounts of deposits, advances, services of remittances, etc.) catered by the bank

- IT Security Organization in Bank

  It talks of the IT security organization – whether it exists and if yes, what is the size, role and sophistication.

- Agility in Business Processes

  This aspect tells us about the need (and related efforts, too) about reducing the time-to-market of new services/products.

- Regulator Directives

  It relates to directives and guidelines from the
regulating agencies, viz. RBI and related strictness and elaborateness.

8.6.3 Tech Deployment

- Tech Sophistication (Vertical)

This factor indicates the bank’s info-tech superiority in terms of latest technologies and complexity & coverage of applications.

- Tech Spread (Horizontal)

It indicates the proportion of the tech-equipped branches to total branches and IT-enabled business to total business.

- Tech Level of Business Partners

This parameter points to IT sophistication of business partners of the bank and also the bank’s technical service providers.

- Multiple Delivery Channels

This indicates the multiplicity of delivery channels, e.g. ATMs, tele-banking, kiosks, mobile-banking, Internet Banking, etc.

- Tech Attacks from Outside

This discrete factor talks about count and complexity of
cyber attacks world over and also those witnessed by the bank.

8.7 This model could be visualized as a 3-D cube with its above three dimensions as (a) Banking Paradigm, (b) Tech Deployment, & (c) Human Dynamics.

8.8 Each of these three dimensions has five factors each making in all fifteen factors as enumerated in the earlier section. There are further issues of these fifteen factors (viz. calibration, interdependencies, mapping of training aspects that are affected) that are developed in the next few sections.
8.9 Following table takes ahead this set of fifteen parameters to assign a codifications scheme for future reference, to explain how the calibration for each is intended and to mark their nature (as internal or external).

<table>
<thead>
<tr>
<th>Class of Causal Factors</th>
<th>Code</th>
<th>Factor influencing Training</th>
<th>Quantifiable / Judgmental</th>
<th>Internal / External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Dynamics</td>
<td>H 1</td>
<td>Total Workforce</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>H 2</td>
<td>Technical Awareness</td>
<td>Judgmental</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>H 3</td>
<td>Work Quantum / Load</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>H 4</td>
<td>Cyber Crime Techniques</td>
<td>Judgmental</td>
<td>External</td>
</tr>
<tr>
<td></td>
<td>H 5</td>
<td>Staff Turnover (Within &amp; Out)</td>
<td>Judgmental</td>
<td>Internal</td>
</tr>
<tr>
<td>Business Paradigm</td>
<td>B 1</td>
<td>Branch Spread / Network</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>B 2</td>
<td>Business Volume</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>B 3</td>
<td>Bank’s IT Security Orgn.</td>
<td>Judgmental</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>B 4</td>
<td>Agility in Business Process</td>
<td>Judgmental</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>B 5</td>
<td>Regulator Directives</td>
<td>Judgmental</td>
<td>External</td>
</tr>
<tr>
<td>Tech Deployment</td>
<td>T 1</td>
<td>Tech Sophistication (Vertical)</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>T 2</td>
<td>Tech Spread (Horizontal)</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>T 3</td>
<td>IT Level of Business Partners</td>
<td>Judgmental</td>
<td>External</td>
</tr>
<tr>
<td></td>
<td>T 4</td>
<td>Multiple Delivery Channels</td>
<td>Quantifiable</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>T 5</td>
<td>Tech Attacks from Outside</td>
<td>Judgmental</td>
<td>External</td>
</tr>
</tbody>
</table>

Table 17: Model Development – Causal Factors & Their Dimensions

8.10 All the fifteen factors are currently considered judgmental. They would be bifurcated as judgmental or quantifiable, and would be
calibrated on suitable scale (say, a ten-point scale) as a future enhancement of the current research.

8.11 Due to their very nature H4, B5, T3 and T5 are external factors, where the bank would be justified to keep an ear to earth to sense, as early as possible, the changes in the business environment, industry trends and technical advancements.

8.12 Before proceeding to trace the influence of each of the above 15 factors on the subject matter of IT security training, it is necessary that impacted six factors are crystallized and enlisted as under:

- Training Coverage (TC) This aspect talks of the complete training coverage as broken up in different modules (about 75 modules are enlisted in the annexure)

- Module Granularity (MG) This is sheer magnitude of the training module also called granularity that helps decide how much time and efforts go into delivery of a module.

- Agility of Training (AT) It denotes the need for swiftness in designing each module (and quickness in delivery for all the audience) that is essential in today’s fast-paced world
- Outreach / In-campus (OI)  It weighs whether the trainer should reach out to audience at their place, Or the participants to travel to training campus.

- Faculty Mix (FM)  This is about determining the match & mix of internal & external faculty and the count needed to cope with size & contents.

- Delivery Methods (DM)  It is an approach of training i.e. conceptual inputs, cases, brainstorming, assignment, quiz, and also e-Learning tools like PC games, Intranet based contents, etc.

8.13 Diagrammatically, the set of influencing factors (causes) can thus be seen along with its six impacted aspects of training as under:
At this stage, it will be proper to demonstrate how the fifteen causal factors influence the six training factors (effects). The full description of the same is provided just after that Cartesian style fifteen-by-six matrix in the next section to represent the complete causal analysis.
Table 18 : Model Development – Impact of Causal Factors on Training

8.15 Here is an account of how the said fifteen causes influence the training in the said six effect areas. Only the ‘High’ and ‘Mid’ impacts are considered:

8.16 Impact on Training Coverage (TC)
• High Impact of H2 on TC  Lesser the IT awareness, more the need for IT security inputs

• Mid Impact of H4 on TC  If the cyber crime techniques are complex and high in number, more inputs will be needed

• Mid Impact of T1 on TC  Higher the IT sophistication, more the need for conceptual inputs o IT security

• Mid Impact of T3 on TC  If business partners have sophisticated IT deployment, the bank needs to train its people commensurately to monitor it

• Mid Impact of T4 on TC  A bank having variety of service channels needs to explain flip side of security hassles to its staff

• Mid Impact of T5 on TC  In case the bank witnesses outside attacks, more and better training inputs serve as an effective preventive control

8.17  Impact on Module Granularity (MG)

• High Impact of H3 on MG  If the staff is loaded with huge work pressures, the module granularity should be relatively smaller, so that program could be pre/post fixed to the daily chore without disturbing the work
8.18 Impact on Agility in Training (AT)

- **High Impact of B4 on AT**
  Agility in business process has an obvious direct impact on the agility needed for IT security training.

- **Mid Impact of T4 on AT**
  As delivery channels are swift in their nature and at times unmanned, the training has to be fast paced.

8.19 Impact on Outreach / In-campus (OI)

- **High Impact of H1 on OI**
  Larger the workforce, more the need for outreach programs to ensure security message is sent thru.

- **High Impact of H3 on OI**
  IF the staff is burdened under work pressure, outreach is the only hope to disseminate the security training.

- **High Impact of B1 on OI**
  If branch spread is far and wide, the outreach is a logical corollary.

- **Mid Impact of B2 on OI**
  For high volume of business, the outreach programs are more suited.
irrespective of whether it is IT security or something else.

- Mid Impact of T1 on OI: In case the tech sophistication is high, the outreach program is enabled as IT could be thought as enabler factor.

8.20 Impact on Faculty Mix (FM)

- Mid Impact of H1 on FM: Larger the workforce, more the need for external faculty support to cope with the training volume
- Mid Impact of H5 on FM: Same as above
- Mid Impact of B1 on FM: If branches are far flung, the external support for training is quite helpful
- Mid Impact of B3 on FM: A bank with IT security organization is better suited to handle training on its own
- Mid Impact of T1 on FM: For cutting edge technology, the bank may not have in-house expertise needed for training
- Mid Impact of T5 on FM: In case there are some outside attacks, the bank would be justified in outsourcing the IT security training due to dire need for expertise
8.21 Impact on Delivery Methods (DM)

- Mid Impact of B1 on DM  For a large workforce, the delivery methods of e-Learning could help to boost the speed

- High Impact of T1 on DM With higher IT sophistication, the bank can think of using hi-tech means for training delivery

- Mid Impact of T2 on DM If the technology has a wide spread, the training methods even in outreach program might be sophisticated

- Mid Impact of T4 on DM With multiple delivery channels, the delivery methods could be equally hi-fi to exploit the bank’s IT excellence

8.22 Now, we come to the interplay of the causal factors among themselves. Such aspects, at least to a certain degree, impact one another and thus in turn underline the need for an iterative computation of the overall impact. Similarly, the interplay of the effects as well is described in the subsequent section. It is this interplay – whether among causes or effects – that makes the model iterative in its nature and calls for certain adjustments as it passes through three distinct cycles before actually arriving at the requisite training design.
### Table 19: Model Development – Interplay of Causal Factors

**Legend**
- **D**: Direct Major influence …… 8 such points explained in next section
- **I**: Inverse Major influence ….. 3 such points explained in next section
- **m**: minor Influence, hence ignored
- **X**: Not Applicable

<table>
<thead>
<tr>
<th>↓ Influencing Factor ↓</th>
<th>← Influenced Factors →</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Human Dynamics</td>
</tr>
<tr>
<td></td>
<td>1   2  3  4  5</td>
</tr>
<tr>
<td>H 1 Total Workforce</td>
<td>X   m</td>
</tr>
<tr>
<td>H 2 Technical Awareness</td>
<td>X</td>
</tr>
<tr>
<td>H 3 Work Quantum / Load</td>
<td>X</td>
</tr>
<tr>
<td>H 4 Cyber Crime Techniques</td>
<td>X</td>
</tr>
<tr>
<td>H 5 Staff Turnover (Within &amp; Out)</td>
<td>m m</td>
</tr>
<tr>
<td>B 1 Branch Spread / Network</td>
<td>m I</td>
</tr>
<tr>
<td>B 2 Business Volume</td>
<td>m   m</td>
</tr>
<tr>
<td>B 3 IT Security Organization in Bank</td>
<td>m</td>
</tr>
<tr>
<td>B 4 Agility in Business Processes</td>
<td>m</td>
</tr>
<tr>
<td>B 5 Regulator Thumping</td>
<td>m   m</td>
</tr>
<tr>
<td>T 1 Tech Sophistication (Vertical)</td>
<td>m m m</td>
</tr>
<tr>
<td>T 2 Tech Spread (Horizontal)</td>
<td>m m m</td>
</tr>
<tr>
<td>T 3 Tech Level of Business Partners</td>
<td>m m m</td>
</tr>
<tr>
<td>T 4 Multiple Delivery Channels</td>
<td>m I</td>
</tr>
<tr>
<td>T 5 Tech Attacks from Outside</td>
<td>m</td>
</tr>
</tbody>
</table>
8.23 Details about Influence mentioned in the table of earlier section

- Influence of H4 on T5  Cyber crime techniques have an obvious direct impact on outside Tech attacks.
- Influence of B1 on H2  More the Branch spread, more the trouble in spreading IT Sec awareness.
- Influence of B1 on B4  More the Branch spread, less agile the business processes as natural outcome.
- Influence of T1 on B3  IT sophistication underscores the need for the Bank’s IT security organization
- Influence of T1 on T3  Tech level of business partners needs to be high to support and / or utilize high-tech banking services
- Influence of T1 on T5  Any system that gets more and more intricate becomes equally delicate, too, thus attracting attacks due to more tendency of inherent flaws
- Influence of T4 on H3  As the bank puts more delivery channels, the work load on the staff starts decreasing proportionately.
- Influence of T4 on B3  Multiple service channels imply necessity of the bank’s IT security organization to safeguard its interests
• Influence of T4 on B4  Diversified delivery channels enable the bank to ensure swiftness in its process changes focusing customers, due to high, widespread automation

• Influence of T4 on T1  Multi-delivery channels pre-suppose (as well as impact, too) the tech sophistication of the bank

• Influence of T4 on T5  Clearly, the variety of delivery channels would attract the proportionate attacks from outside

Interestingly, some of the above causal relations may not be emerging clearly for the bank, as the reasons may be latent without actually springing up in action. Nonetheless, the bank needs to take into account these ripple effects.

8.24 Now, we come to the interplay of the resultant factors (effects) among themselves.

• Interplay between TC on MG Training contents is a superset, while the module is a subset. Hence the two are inter-related

• Interplay between TC on AT Size of the Training contents will have an inverse impact on agility in training
• Interplay between TC on FM  Training contents will impact the faculty mix due to its size and intricacy, whereas contents will get impacted based on who teaches the course.

• Interplay between TC on DM  Contents will have a direct linkage to the delivery methods of cases, practical, etc.

• Interplay between MG on OI  Smaller the module granularity, easier it is to engage it in-the-field

• Interplay between MG on AT  Smaller the granule size, faster the pace of training

• Interplay between OI on FM  When it comes to outreach and faculty mix, the two issues are intimately related to each other for obvious reasons

• Interplay between OI on DM  Outreach programs may have limitations on delivery methods due to infrastructural constraints

• Interplay between DM on AT  Delivery methods like e-Learning are agile, whereas the brainstorm methods would be bit lengthy
8.25 Need for the iterative process will be now clear. Here are some tips on how the model of IT STCM could be best deployed by taking as many as four passes through it:

- **Pass 1** This is simple fall through IT SITM with no bothering about the interplay of any factors. So, the assessment of all the influencing factors may be done one-by-one to assess their individual impact on six training aspects.

- **Pass 2** Now, the interplay among the fifteen causal factors is to be undertaken, one pair at a time. Each time, it should be followed by the respective refinement in the six training aspects so that the final effect of eddy currents within causal factors is worked out then and there itself.

- **Pass 3** Lastly, the inter-relations among the six training aspects are to be encountered. As the association between each pair is worked out, the resultant adjustment could be noted. Here, care must be taken to ensure that the mutual impact of both the elements in the pair is considered and that one-way evaluation is not performed.

- **Pass 4** As a confirmatory test it would be essential to check that neither something is missed out, nor something is given double or more weightage. Thus in the fourth
pass, all the steps will be re-run to re-check the earlier working and wherever necessary, the corrections could be made.

8.26 As a recapitulation, the following diagram – the final and fully unfurled version of the IT STCM – is presented here.

8.27 Experimental Application of the Model

While the IT STCM was getting developed and thus was still in fluid mode, the researcher had an opportunity to try it out – in part, though – on experimental basis for few banks like Corporation Bank, Bank of Maharashtra, Bank of India, Karnataka Bank, State
Bank of India, etc. The most significant experiment was for the largest public sector Indian bank – State Bank of India.

8.28 Before narrating further details, it is clarified that the IT STCM could not be fully applied, at it was evolving. Nonetheless, the major components of the model, i.e. 15 influencing factors and 6 impacted factors, were certainly taken into account. What was not tried is the iterative process of inter-dependent factors.

8.29 To start with, here is how the impact was assessed, for State Bank of India.

(i) Impact of High IT sophistication (T1) on Trg. Coverage (TC)
   - Application Bank’s usage of Digital Signatures guided inclusion of Asymmetric Key Encryption; usage of Network management system (NMS) implied inclusion of network security issues, Intranet & Internet deployed at Branches suggested coverage of Web & Email security issues, etc.

(ii) Impact of business partners’ IT sophistication (T3) on Trg. Coverage (TC)
   - Application Bank with its asset base of over 4.5 lakh crore has lot many Service Providers for Internet, Facility Maintenance, Anti-Virus, ATM upkeep, etc. are hi-tech companies hence outsourcing
risks and remote access concerns were included in training coverage

(iii) Impact Various service channels (T4) on Trg. Coverage (TC)

○ Application Internet security was planned in training due to Internet Banking; special module on ATM security included as bank has a base of over 3500 ATM’s

(iv) Impact Agility in Busi processes (B4) on Agility in Trg. (AT)

○ Application Bank has been driving aggressive marketing strategy through its fast transformation of business processes across its 9000 branches. This had a clear implication on compact modules to be deployed on need-basis for various target audiences

(v) Impact Agility in busi process (B4) on Agility in Training (AT)

○ Application As explained earlier, the Bank has geared up pace of its business processes transformation. So, similar swiftness is planned in IT security training through several steps of ready-made courseware, Train-The-Trainers programs, etc. as explained later.
(vi) Impact Variety of delivery channels (T4) on Agility in Training (AT)

- Application Rich variety of delivery channels has demanded substantial speed of security dissemination and has been tackled through various steps as explained in the last section.

(vii) Impact of Large workforce (H1) on Outreach / In-campus (OI)

- Application Large workforce of over 2 lakh has guided to utilize the approach of outreach programs in the field through 50+ training centers of the bank.

(viii) Impact of Branch spread (B1) on Outreach / In-campus (OI)

- Application As the branch spread is over 9000, the extension programs in the field are absolutely essential.

(ix) Impact of Large workforce (H1) on Faculty Mix (FM)

- Application Due to the monolith size of staff strength, the external faculty has been roped in. Besides, the Train-The-Trainees programs have also been adopted to build up bank’s own team of trainers.

(x) Impact of Cutting edge technology (T1) on Faculty Mix (FM)

- Application Due to hi-tech deployment in the bank, external faculty has been sought for complicated topics,
whereas the internal faculty conducts relatively simple training on IT security

(xi) Impact of Large workforce (B1) on Delivery Methods (DM)
   o Application Huge worker strength has guided that mixed delivery methods of classroom sessions plus e-Learning be adopted. Hence, PC based Games deployed with great success.

(xii) Impact of Higher IT sophistication (T1) on Delivery Methods (DM)
   o Application As hi-tech IT deployment is in existence, the delivery methods of computer-based training (CBT) and web-based Training (WBT) could be thought of.

8.30 To sum up, here is the list of the resultant steps taken for IT security training in respect of State Bank of India (and few others also, mentioned below), as transformed through IT STCM:
   • Distinct Modules for Specific Audiences (SBI, Corp Bank)
     o Top Executives, IT Specialist Officers, Trainers, etc.
   • External Faculty Support (Bank of India, Bank of Maharashtra)
     o External support from the researcher was sought not only for delivery of star sessions but also on the issues
of how to quickly transform the whole process, the training modalities for subsequent batches, etc.

- Ready-built Courseware (Corp Bank, Allahabad Bank)
  - A rich set of courseware was also invited from the researcher. It included powerpoint slides, reading notes, DO’s and DON’Ts, quizzes, case studies, etc.

- PC Games (Syndicate Bank, SBI)
  - A set of PC games were deployed as a part of the IT security training to draw on the advantages stated in section 4.4.

- Train-The-Trainers (Karnataka Bank, SBI)
  - This was a notable step advanced by these banks (SBI, the largest bank with workforce of over 2 lakh spread over 9000 branches and Karnataka Bank, a compact private bank with about 4,500 staff strength across 400 branches). Several batches of this specially designed program were held by the researcher to enable the bank’s 50+ faculty members drawn from various regions.

- Outreach Programs (Corp Bank, SBI)
  - Researcher himself conducted the programs at Mumbai, Hyderabad, Bangalore, Mangalore, etc. Besides, the bank’s trainers have been multiplying such batches
across length and breadth of the nation for their colleagues at branches.

- Agility in Training (State Bank of India)
  - It is remarkable swiftness that IT security training for the Top Executives and IT specialist officers, as also multiple batches for Train-The-Trainers program were accomplished within flat two months period.

8.31 Researcher is aware of limitations in these past implementations of IT STCM like partial usage, judgmental assessments, lack of quantified data, etc. that are planned to be taken up for more rigorous experimentation in the post-doctoral research.

8.32 At the end of this chapter, implementation guidelines for the IT STCM model are provided in the next few pages.
Guidelines on How to deploy the IT-STCM model

8.33 IT Security training is an arduous task that calls for thorough training need analysis, module & courseware design & careful delivery of the training programmes. The model devised by the researcher – IT-STCM – could come handy to perform all these tasks in a methodical manner, as explained in the following guidelines.

8.34 The model embraces 15 Major contributory factors (causes) that influence the IT security training and 6 Key impacted factors (effects) of IT security training that are influenced by the said fifteen causes.

8.35 These causes and effects are explained in the next few steps. Anyway, before delving into that, it is essential to think of tailoring the model, if necessary. The model is open-ended and customizable to certain extent, in that the list of 15 causes and / or 6 effects could be modified marginally to include / exclude some of the items as might be guided by the organization-specific IT paradigm.

8.36 Next, the calibrations for each of the causes and effects should be performed to arrive at the training design. Wherever relevant, the whole process may be iterated to fine-tune for the interplay of
the causes and / or effects among themselves should be taken into account when using the model.

8.37 This complete simulation is recapitulated by way of a structured check-list as under.

- **Step 1** Assign the weightages to each of the fifteen causes by carefully studying the organization’s prevalent IT deployment, business scale and the workforce.

- **Step 2** Assign the weightages to each of the six effects after critically evaluating the capabilities and maturity of the training function in the organization.

- **Step 3** With the table 18 depicting the High, Mid and Low impact ratings as the base, tailor the impact of 15 causal factors on six training aspects, by adjusting the ratings, wherever deemed fit.

- **Step 4** Take a gist of each of the six columns of the table – one each relating to six training aspects – and ascertain the primary impact on the form / contents for each of them.

- **Step 5** Evaluate the interplay among the fifteen causal factors, one pair at a time, and carry out at the refinements, if any.
Step 6. Loop back to the step 3 in the light of revised ratings of the fifteen causal factors as done in the previous step. The cycle continues till there are no changes needed at table 18.

Step 7. It is now logical to assess the inter-relations among the six training aspects. Here, care must be taken to ensure that the mutual impact of both the elements in the pair is considered and that one-way evaluation is not performed.

Step 8. Revisit the step 1 to weed out the disproportionate ratings, if any, to the fifteen causal factors.

Step 9. Revisit the step 2 to even out the inconsistencies, if any, in the allocations of six training aspects.

Step 10. Simulate through steps 8 and 9, till you come to a constancy for all the twenty-one elements, that merit no more revision any further.
This check-list could also be depicted as a flow chart as under:

**Figure 57: Flow Chart showing implementation of IT STCM model**
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 blindened 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 form 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.