Chapter 2. Research Background

This chapter narrates the reasons why the researcher was prompted to undertake this research. Broadly stated, it was his consulting for a variety of Indian banks from all walks (viz. public, private and cooperative sector) that conjured up a notion of an adhocism in IT Security training, which in turn called for a systematic and objective treatment to the topic.
2.1 In the capacities of consultant, trainer and auditor, the researcher has been interacting on the topic of IT Security with several bankers at all levels of organizational ladder, from all walks of Indian banks, for over a decade.

2.2 This offered the researcher repeated opportunities to gauge the IT security by way of

A) Interaction with a cross section of workforce of banks including
   a. Mainstream bankers at grass roots of branches
   b. Support professionals at branch level
   c. IT Officers monitoring computerization of a few branches
   d. Inspecting / Auditing Officials examining the branches
   e. Security Officers looking after physical security
   f. IT Head at Central offices of the Banks
   g. IT Security Head (wherever designated) ay Central Offices
   h. Heads of Departments at Central Offices of Banks
   i. Top Executives in charge of general management

B) Observing the IT security efforts by the banks, in terms of
   a. IT Security Organization
   b. IT Security Policy
   c. Disaster Recovery Plan / Business Continuity Plan
   d. Automated IT Security tools like firewalls, etc.
e. IT Security practices at branches and other offices

f. Concerned documentation

2.3 A sort of adhocism or lack of orderly endeavour was experienced in the training plans & efforts of several banks, as could be seen from following subtle observations

A) Unlike other corporate training exercise, IT security training efforts seemed to have missed out on
   a. Initiation of the process before hand for the whole year
   b. Careful planning about target audience: cadres & counts
   c. Organizing the faculty, coordination, batches, schedule.
   d. Budgeting for the fees, infrastructure and courseware

IT security training is more or less conducted on the spur of moment, without advance planning or later monitoring.

B) In some cases, even the IT Heads were observed to be not so well equipped on IT security matters, as they probably lacked
   a. Working Skills of IT security
   b. Capability to design any IT security program
   c. Evaluation & Recommendation of security solutions
   d. Awareness about latest updates on recent security threats
   e. Keeping abreast with the IT security research
These IT executives were, dismal to mention, more guided by the security product vendors and security service providers and less studied / equipped.

C) For most of the training heads, the trends and patterns in training were obviously very well known, but the IT security training appeared to be a weak link for them, as under:
   a. IT Security appears to be a totally foreign subject to them
   b. Resulting invariable reliance on IT department about
      i. Not just content and courseware,
      ii. but also for training methods, duration, audience
   c. Inability to independently / collaboratively tackle
      i. Training needs of IT security across various roles
      ii. Module Design for the respective roles
      iii. the seriousness and sense of proportion of topic

D) A casual talk with staff at bank branches discloses that this cutting edge (i.e. public facing), where the IT security impact and awareness should be clearly palpable, is so much tied down with their routine daily chore that in most of the cases, they do not have adequate IT awareness to efficiently handle the deployed IT, let alone the intricacies and real significance of the IT security.
E) Lack of IT security awareness has resulted into following serious lacunae among the rank and file

a. Top Executives Compliance stressed, security reviews / strengthening trivialized

b. Training Head IT security is made mockery in keynote address that demoralizes people

c. IT Officers Security hardening delays that invites hackers indirectly

d. Branch Staff Ignorance is bliss and half knowledge is dangerous

Besides, the common symptoms of IT security across all rungs have been (i) security superstition about brands, (ii) Role of IT as enabler is harped on, countering concerns are ignored, (iii) a wishful thinking that security mishaps won’t happen here.

F) All these observations got more and more firm during some 50 training programs engaged by the researcher, where he interacted with over 1000 participants from across 25 different banks. This banking cross section of Indian banks confides with a thumping majority the singular fact: The dire need of training inputs for bankers to bring their IT security awareness to a threshold level.
2.4 Some glaring points of ignorance are narrated here to offer a feel of the severity of the problem:

A) No inkling about Existence of following major documents
   a. Bank’s IT security policy
   b. Bank’s Disaster Recovery Plan / Business Continuity Plan
   c. Information Technology Act, 2000

B) Lack of Working knowledge of
   a. Passwords
   b. Backup
   c. Banking software parameter settings

C) Not even Sketchy Idea about
   a. Hacking Attacks
   b. Email Frauds
   c. Digital signatures

2.5 Based on above, it was surmised that there is considerable scope to bring about a systematic approach to the IT security training in Indian banks, with major points wanting, as under:

A) Baseline of IT Security awareness among the staff is not assessed in a systematic manner with necessary consideration for employee-mix and their respective roles and responsibilities
B) Adequate exercise is not done on the vision – the expected level of IT Security knowledge the employees in respective strata need to attain in pre-determined time span

C) Training plan do not indicate enough thinking in terms of contents finalization, module design, duration, schedule, participant level, batch size, location, delivery methodology, trainer qualifications

2.6 In few cases, some apprehension was indicated about the degree of effectiveness and smooth IT operations due to absence of sound IT security awareness in the workforce across branches.

2.7 In some other cases, the IT security mishaps came to fore in the course of discussions. The minor ones could be discussed with openness, anyway, the serious ones could be interpreted through the vague and short versions.

2.8 Such perceived feeling (of arbitrary outline of IT Security training and a need for more systematic efforts in that direction) was endorsed and seconded during a few select meetings with couple of veterans – from both walks viz. the banking and the IT – based on their gut-feeling and experience.

2.9 In the field of IT, the phenomenon of ‘moving targets’ is applicable to training, too; therefore Deming’s cycle of plan-do-check-act befits IT security training that has to be continually monitored for
its design, delivery, effectiveness and refinement in the light of ever-changing scenario of IT and IT security.

2.10 It is this surmise of inadequate design of the IT Security Training (and obviously its impact on efficacy of such training) that is to be confirmed with this systematic study.