Chapter 4. Secondary / Literature Survey

This chapter provides an account of scanning and searching of related past works in print form and electronic form of websites. This went in a cyclical manner, as one triggered other. The researcher presents here his train of thoughts that string together the references coherently across four broad sub-sections, viz. 4.1 Indian Banking, 4.2 IT Security, 4.3 Training, and 4.4 Experience Survey.
4.1 **Indian Banking**

4.1.1 Banking is defined by section 6 of the Banking Regulations Act as 'Accepting, for the purpose of lending or investment, of deposits of money from public, repayable on demand or otherwise, and withdrawable by cheque, demand draft, order or otherwise'.

4.1.2 Banking goes much beyond this simplistic definition and serves as a very crucial constituent of Economics. It helps a layman to keep aside a part of his earning as savings, then aggregates such savings into a sizeable quantum, deploys these funds through profitable means of investments & advances and thus ensures the circulation of funds to boost the nation’s economy.

4.1.3 India is no exception. Indian Banking has been contributing its might by imbibing habit of savings among public, canalizing these funds for productive ends and helping the whole society to manage its funds.

4.1.4 Besides, there are certain ancillary services like remittance of funds, locker and safe custody facilities, non-fund based offerings like bank guarantees, solvency certificates & letter of credits.
4.1.5 In addition, banks also extend merchant banking consulting to the corporate sector, executor and trustee services to trusts and foundations and de-mat services to individual investors.

4.1.6 While this fundamental nature and framework of banking has been consistently the same across decades, a noticeable transformation has been taking place in the other banking services, tools, forms, ways and volume that all have undergone a sea change in last few decades.

4.1.7 The Reserve Bank of India — the central bank of our country — monitors the functioning of all the Indian banks that are classified as public sector banks, private sector banks, cooperative banks, regional rural banks, etc.

4.1.8 At this point, it would be fit to look into the wide variety in Indian banking on the parameters stated below:

A) Constitution

There are multiple organizational varieties, viz. public sector banks (e.g. Syndicate Bank), private sector banks (e.g. UTI Bank), cooperative banks (e.g. Janata Sahakari Bank) and regional rural banks (e.g. Buldana Gramin Bank), etc.

B) Scale

Business volumes indicate a wide spectrum of small banks having a limited size of just few
crores, right up to giant banks with volume of few lakh crores.

C) Spread

Broad spectrum of expanse and penetration ranges from banks having branch count in single digit and extends to colossal banks having nearly ten thousand branches, distributed across length and breadth of our nation.

D) IT Deployment

While some banks are yet toying with an idea of procuring the first ever computer, some others have a comprehensive, complex and costly IT infrastructure catering to absolutely every single banking need and use of IT even as a strategic tool for business.

The researcher had to face an arduous task of taking all these varieties in consideration and to come up with a common denominator for all of them.

4.1.9 There have been many major milestones in Indian banking:

A) Government emphasized a social control over banks in mid sixties by delineating the control nexus between industries and banking dominated by industrialists.
B) Nationalization of 14 major banks in 1969 followed by expansion of branch network in rural and semi-urban areas to span the length and breadth of the nation

C) Another spell of nationalization of batch of 6 more banks in 1980 to strengthen the government’s propositions. This made the PSU banks the major component in Indian banking though some relatively banks continued to be private

D) Re-orienting these nationalized banks towards common man by putting some targets of priority sector lending, thus making the ‘purpose’ as a new yardstick for lending, dislodging sound criterion of ‘security’ or the property that could be charged

E) Early nineties saw the pendulum swinging back with government giving a nod to private sector’s entry in banking with opening up of new generation private banks.

F) Cooperative banks continued their overall working in a relatively undisturbed manner, except that the new genre of regional rural banks were brought in to serve rural populace.

4.1.10 This all din and turmoil has several significant impacts. Of these, the relevant for the current study are massive expansion of bank branches across our nation, tremendous growth in business volume, growth in the workforce as driving force and the computerization adopted in the whole course.
4.1.11 The growing network of bank branches has today grown considerably with a total count of 68,200 branches. Top three states having maximum branches are

- Uttar Pradesh 8348
- Maharashtra 6590
- Andhra Pradesh 5348

On this backdrop, the least number of branches are located in

- Daman & Diu 16
- Dadra & Nagar Haveli 11
- Lakshadweep 9

The average branches per state / union territory are 1949.

4.1.12 These figures expressed in absolute terms would evince their real significance when expressed in terms of ‘Population served by a bank branch’. Best fit states / union territories are

- Chandigarh 4000
- Goa 5000
- Chandigarh 4000

Those three having not so favourable ratio are

- Tripura 22000
- Nagaland 25000
- Manipur 33000

The average for population per bank branch is 14,660
4.1.13 This network of branches could be viewed on another dimension of the banks’ classification as under:

<table>
<thead>
<tr>
<th>Bank Type</th>
<th>Bank Count</th>
<th>Branch Count</th>
<th>Br’s per Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public sector</td>
<td>27</td>
<td>47,794</td>
<td>1,707</td>
</tr>
<tr>
<td>Private banks</td>
<td>28</td>
<td>6,128</td>
<td>219</td>
</tr>
<tr>
<td>Coop &amp; RRB’s</td>
<td>2300</td>
<td>14,278</td>
<td>6</td>
</tr>
</tbody>
</table>

Figure 1: Average branches per bank

4.1.14 Due to a low ratio of Branches per Bank, many cooperative and regional rural banks have not gone ahead with a computerization program in a big way, as there is neither a pressing need nor the adequate funding for automation initiatives. Besides, a good proportion of them are situated in remote mofusil areas, where the technology penetration in general is meager.
4.1.15 There are anyway some notable exception of bigger banks in urban area from this cooperative and regional rural banks segment that have been included in the research project.

4.1.16 Coming to the transactional workload, it would be pertinent to state the following figures of cheques that are cleared in Indian clearing houses:

<table>
<thead>
<tr>
<th>Year</th>
<th>Count (Million)</th>
<th>Amount (Crores)</th>
<th>Year</th>
<th>Count (Million)</th>
<th>Amount (Crores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984-85</td>
<td>462</td>
<td>457536</td>
<td>1994-95</td>
<td>737</td>
<td>4101079</td>
</tr>
<tr>
<td>1985-86</td>
<td>514</td>
<td>517608</td>
<td>1995-96</td>
<td>759</td>
<td>4624640</td>
</tr>
<tr>
<td>1986-87</td>
<td>645</td>
<td>658008</td>
<td>1996-97</td>
<td>783</td>
<td>5423476</td>
</tr>
<tr>
<td>1987-88</td>
<td>711</td>
<td>724632</td>
<td>1997-98</td>
<td>858</td>
<td>6598150</td>
</tr>
<tr>
<td>1988-89</td>
<td>569</td>
<td>670608</td>
<td>1998-99</td>
<td>866</td>
<td>7576554</td>
</tr>
<tr>
<td>1989-90</td>
<td>590</td>
<td>926174</td>
<td>1999-00</td>
<td>891</td>
<td>9232018</td>
</tr>
<tr>
<td>1990-91</td>
<td>764</td>
<td>2287353</td>
<td>2000-01</td>
<td>941</td>
<td>10747119</td>
</tr>
<tr>
<td>1991-92</td>
<td>868</td>
<td>3404254</td>
<td>2001-02</td>
<td>902</td>
<td>12575254</td>
</tr>
<tr>
<td>1992-93</td>
<td>768</td>
<td>3702008</td>
<td>2002-03</td>
<td>1014</td>
<td>13424313</td>
</tr>
<tr>
<td>1993-94</td>
<td>761</td>
<td>3868913</td>
<td>2003-04</td>
<td>1023</td>
<td>11594976</td>
</tr>
</tbody>
</table>

Table 4: Volume of Cheques cleared by Indian Banks
4.1.17 In terms of business volume handled by Indian banks, that is also worth mention. Assets of the Indian banking show a staggering figure of Rs. 20,000 billion and the detailed breakup of these assets with a comparative annual growth is as under:

<table>
<thead>
<tr>
<th>Year (end-March)</th>
<th>Assets (Rs. In Crore)</th>
<th>Total Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cash and Balances</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With RBI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bal with Banks &amp; money at</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Short notice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>1990-91</td>
<td>35991</td>
<td>172849</td>
</tr>
<tr>
<td>1991-92</td>
<td>35474</td>
<td>208818</td>
</tr>
<tr>
<td>1992-93</td>
<td>39463</td>
<td>248726</td>
</tr>
<tr>
<td>1993-94</td>
<td>51561</td>
<td>262601</td>
</tr>
<tr>
<td>1994-95</td>
<td>63049</td>
<td>290638</td>
</tr>
<tr>
<td>1995-96</td>
<td>70194</td>
<td>315570</td>
</tr>
<tr>
<td>1996-97</td>
<td>60929</td>
<td>318538</td>
</tr>
<tr>
<td>1997-98</td>
<td>71590</td>
<td>324166</td>
</tr>
<tr>
<td>1998-99</td>
<td>81384</td>
<td>369271</td>
</tr>
<tr>
<td>1999-00</td>
<td>84927</td>
<td>444124</td>
</tr>
<tr>
<td>2000-01</td>
<td>84503</td>
<td>526150</td>
</tr>
<tr>
<td>2001-02</td>
<td>86760</td>
<td>564537</td>
</tr>
<tr>
<td>2002-03</td>
<td>86122</td>
<td>639553</td>
</tr>
<tr>
<td>2003-04</td>
<td>113245</td>
<td>864142</td>
</tr>
</tbody>
</table>

Table 5 : Assets of Indian Banks
4.1.18 Out of these assets of Rs. 19,75,918 Crores, Rs. 14,71,077 Crores are owned by 28 public sector banks while Rs. 4,25,802 Crores are owned by 28 private banks, leaving a small pie of hardly about Rs. 1,00,000 Crores that is owned by about 200 regional rural banks and approx. 2000 cooperative banks together. This scenario could be graphically represented as under:

**Relative Position of Assets of Banks**

<table>
<thead>
<tr>
<th>Type of Bank</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSU Banks</td>
<td>74%</td>
</tr>
<tr>
<td>Private Banks</td>
<td>21%</td>
</tr>
<tr>
<td>Coop + RRB</td>
<td>5%</td>
</tr>
</tbody>
</table>

Figure 2 : Relative Position of Assets of Indian Banks

This major share of the public sector and private sector banks was one of the factors behind the decision to confine this study to those banks only.
### 4.1.19 Corresponding snapshot of liabilities is presented below:

<table>
<thead>
<tr>
<th>Year</th>
<th>Liabilities (Rs. In Crore)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Capital</td>
<td>Reserves &amp; Surplus</td>
</tr>
<tr>
<td>1990-91</td>
<td>3069</td>
<td>3171</td>
</tr>
<tr>
<td>1991-92</td>
<td>4053</td>
<td>4994</td>
</tr>
<tr>
<td>1992-93</td>
<td>4858</td>
<td>6639</td>
</tr>
<tr>
<td>1993-94</td>
<td>10544</td>
<td>11474</td>
</tr>
<tr>
<td>1994-95</td>
<td>16180</td>
<td>15673</td>
</tr>
<tr>
<td>1995-96</td>
<td>16347</td>
<td>20521</td>
</tr>
<tr>
<td>1996-97</td>
<td>16577</td>
<td>27187</td>
</tr>
<tr>
<td>1997-98</td>
<td>19439</td>
<td>34003</td>
</tr>
<tr>
<td>1998-99</td>
<td>18265</td>
<td>36735</td>
</tr>
<tr>
<td>1999-00</td>
<td>18435</td>
<td>43451</td>
</tr>
<tr>
<td>2000-01</td>
<td>19094</td>
<td>48645</td>
</tr>
<tr>
<td>2001-02</td>
<td>21472</td>
<td>62683</td>
</tr>
<tr>
<td>2002-03</td>
<td>21594</td>
<td>76288</td>
</tr>
<tr>
<td>2003-04</td>
<td>22348</td>
<td>94240</td>
</tr>
</tbody>
</table>

Table 6: Liabilities of Indian Banks

### 4.1.20 Taking this business volume and relative share of public and private banks ahead, here is an interesting comparison of their key indicators of business
<table>
<thead>
<tr>
<th>Key Indicator</th>
<th>Private Banks</th>
<th>Public Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>4,25,802</td>
<td>14,71,077</td>
</tr>
<tr>
<td>Deposits</td>
<td>3,12,645</td>
<td>14,35,853</td>
</tr>
<tr>
<td>Investments</td>
<td>1,38,968</td>
<td>6,85,729</td>
</tr>
<tr>
<td>Advances</td>
<td>2,20,337</td>
<td>8,54,671</td>
</tr>
<tr>
<td>Expenses</td>
<td>24,795</td>
<td>1,05,291</td>
</tr>
<tr>
<td>Op. Profit</td>
<td>7,668</td>
<td>39,052</td>
</tr>
<tr>
<td>Branches</td>
<td>6,128</td>
<td>47,794</td>
</tr>
<tr>
<td>Staff</td>
<td>92,411</td>
<td>7,48,711</td>
</tr>
</tbody>
</table>

Table 7: Private & Public Sector Banks – Comparative Position

4.1.21 On the backdrop of the last section narrating the overview of Indian banking, it will be now in the fitness of things to consider various reasons behind the computerization in this vital sector of economy before moving to automation initiatives in the next section.

A) Growing Volume of Business

It is illustrated in the earlier section how the banking has shown manifold growth in past few decades. On whatsoever dimension – may it be bank count, branch count, total working funds, per branch business, per head operations, etc. – the Indian banking has progressed in a massive way, necessitating the need for deployment of IT.
B) Complexity of Banking Operations

Banking that started with simple deposits and advances has now embraced business diversions like bancassurance where insurance policies are sold by bankers, merchant banking operations where public issues of capital are managed on behalf of corporate world, and many more. Even within core functions of deposits, there have been intricacies like flexi-fixed deposits, where the fixed deposit of a customer could be liquidated, partly or fully, to honour his cheques. All these complexities imply the need for automation.

C) Competition Pressure from Peers

New genre of private sector banks have brought the new wind of sophistication in Indian banking. As these banks exhibited a high degree of smooth and simplified services, the banks from all walks have experienced an urge to win the new customers and to retain the old clientele so as to stay in the business race.

D) Cost per Banking Transaction

With IT deployment, the cost per transaction descends dramatically, inasmuch as it is at least hundred rupees per transaction across the counter, around ten rupees for an
ATM transaction and hardly a rupee for an Internet transaction.

It will be pertinent to mention that these costs are indicative and dependent on the business volume that has to reach a certain critical mass.

E) Phenomenal Rise in Branch Network

The growth of Branches of Indian banks has shown an unparalleled trend since nationalization in 1969. Moderate branch count of Indian banks in the pre-nationalisation era has undergone a three-fold growth to stand at a colossal figure of 68,200 branches as at end of financial year 2004-05.

F) Need for Tighter House keeping

Another concern for banks has been maintaining the house in
order. With a plethora of services, gargantuan accounts and staggering balances across all branches, banks realized that process automation is necessary for internal accounting.

G) Swift Remittances of Funds

With liberalization of economy and globalisation trends, the bank customers have got in touch with their business associates across different continents and also seen the functioning of the banks abroad. Naturally, these customers have been more demanding the effective and efficient banking services, on par with the foreign banks.

H) Linkage with global units like SWIFT

Similarly, during their foreign exchange operations, Indian banks have themselves seen the way international banking deploys the information technology. Besides, some of the international facilitators like Society for Worldwide Inter-bank Financial Telecommunications (SWIFT), Western Union Money Transfer, etc. have been insisting that on Indian Banks should adopt the information and communication technology (ICT) to stay in tune with the global scenario and to transact the business with tech-savvy banks abroad.

I) Customer Service Initiatives

In view of offering better and faster customer service, many
Indian banking have to think of massive automation programs, because unless the customer is served with speed, courtesy and competitive rates, there is every possibility that in this era of free economy and competition, he may turn to some other bank fulfilling his needs.

J) Pressures from Service Providers like ISP

Another sector to boost the computerization in Indian banking has been the various business partners and corporates on Indian scene that has encouraged banks to embark upon computerization programs. Such players include the giant Indian multi-national companies, progressive IT companies like software houses, telecom services providers, etc.

K) Need for Flawless Operations

Over period of time, the banks have witnessed certain degree of errors that creep in their accounting systems for several reasons like manual errors, increased work loads, less time for house keeping, growing pressure on back office operations, not so high work morale and loyalty, trade union activities, etc. All these point to a dire need to adopt automation tools without which the error free working will not be possible given the business volumes to be tackled by Indian banks.
L) Growing Pressure on Profitability

One more pressing issue had been the declined profitability due to reorientation of Indian banks from profits to social service in seventies and eighties. In nineties, the pendulum has started swinging to other end as regulators have started questioning profitability of banks by pushing the social cause to a somewhat back seat. As an aftermath, banks have to deploy computers that would eventually bring down the per transaction cost in banking arena.

M) Speedy Computations of MIS

Equally important point to be noted is the growing pressure on banks to show an adept and agile management information systems (MIS). Few examples here would be complicated schemes of Non Performing Assets (NPA) that is a continually moving target about productivity and profitability of loans and advances portfolio, Tax Deducted at Source (TDS) that is to be deducted on the interest paid to depositor beyond a certain threshold level, etc. Such computations invariably need IT deployment.

No wonder, then that the Indian banks went ahead to adopt the computerization programs to cope with their formidable task.
4.1.22 Banks in India took up the massive computerization program in mid eighties when the committee set up by Reserve Bank of India under the chairmanship of its Deputy Governor Dr. Rangarajan presented a broad outline of the programme.

4.1.23 Automation was in its crawling stage in those days and banks adopted PC with mere floppy drives and later on the PC / XT having hard disk drive. This essentially meant that all computers were in a stand alone mode without any connectivity among them. It had a serious limitation of piecemeal data on each computer, that used to be looked upon as a miraculous monster, quite difficult to tame.

4.1.24 Banking computerization was marked with following factors in those days:

A) Software architecture was more or less mapped on to the ‘counters’ paradigm of banks, i.e. there would be one PC/XT catering one counter related to say savings bank account numbers 1 to 2000, another one for few more thousand accounts that were looked after by another ledger keeper, and so on.

B) The data as well as software on one computer would have no linkage with another. In other words, data & software for each
computer was completely stand alone without any interchange of data by way of cables or disks exchange.

C) IT also meant that the data was stored on a piece meal basis and software would be copied onto each machine with neither advantages nor botherations of connectivity.

4.1.25 By the turn of nineties, the PC / AT and the networking technologies evolved and then banks went ahead with partial branch automation (PBA) program and then with total branch automation (TBA), where almost all the functions like savings bank, Current accounts, Cash credit, etc. were computerized. Slowly but surely the awareness of the bank employees started picking up, however, it was confined to those few who operated the computer. Although the computers within a branch were hooked up together, the branches were still isolated, i.e. the computers in one branch were not connected with the computers of other branch.

4.1.26 At this stage of TBA, the banking computerization exhibited following traits:

A) Instead of earlier scenario of fully stand alone systems, now there was a local area network (LAN) of computers in the bank branch.
B) The file server in this LAN would store the software for all functions and the data across all account types for that branch.

C) This started concentration of data & software from individual counter to a single computer (server) at the branch.

4.1.27 In that era, the IT Security was not even dreamt of by bankers. In the hindsight it was due to three major factors, viz.

A) Fragmented data – It meant that data of each branch was segregated from other branches; Naturally there was no risk perceived due to limited size and scope of the data

B) Lack of interconnectivity – It meant nobody, whether staff or others, could operate the computers at one branch from other branch, thereby confining the span of control to individual branch

C) Low awareness among the public and staff – Given the period of about a decade back, the basic computer literacy itself was too low, let alone the working skills for banking operations or the expertise required for deliberate attacks.

4.1.28 It would also be interesting to note that Internet had then started picking up and hence the security menace of hacking, virus, worms, Trojans, breaking of passwords, etc. was in its
crawling stage as compared to its advanced nature and far &
wide spread today.

4.1.29 Around this period, some banks went ahead with inter-
connectivity among some of the branches. This entailed wide
area network (WAN) to share some data that was needed by
more than one branch – typically the inter-branch transactions, in
a limited way though – for customer convenience and for bank’s
own housekeeping.

4.1.30 At this phase, the banking computerization witnessed following
points:

A) An unprecedented swiftness in the customer service was
made available, particularly for remittances as a limited way
of customer transactions across two branches

B) For the first time some link between banker and customer
went outside the banker’s premises and control, inasmuch as
the vulnerabilities of wire tapping, sniffing and snooping on
the network opened up.

C) The information security was brought to fore as a palpable
factor, in a very miniscule manner though, and bankers
started thinking about it.
4.1.31 During late nineties and early years of the twenty-first century, Indian Banking initiated the concept of anywhere and anytime banking by deploying two revolutionary technologies of:

A) Centralised Banking Solution also known as Core Banking Solution (CBS) where many/all branches of the bank are connected to a central server housing the data of customers of all the branches.

B) Multiple delivery channels – viz. Internet Banking, Automated Teller Machine (ATM), Tele-banking, Mobile-banking – that made it possible for customers to transact the banking beyond four walls of a bank and beyond the office hours.

4.1.32 CBS & ATM was technological leapfrogging that revolutionised customer service and raised it to new heights of customer convenience & delight. Equally, it brought about a paradigm shift in IT security also, for several reasons, as under:

A) ATM witnessed an unprecedented human-less banking, which means the criminals could fiddle with it leisurely without much botheration of getting noticed.

B) CBS, with the data of all customers across all branches of a bank concentrated at a single point, went against the age-old security wisdom of not putting all eggs in one basket.

4.1.33 Two contemporary milestones would be worth noting
A) Y2K – The year 2000 problem commonly known as Y2K was a huge threat looming large on the whole IT world including banking domain, which infused substantial time, energy, funds and manpower to mitigate this issue. After the 21st century began without any hassles, two major afterthoughts came up

  o IT, that seemed to be all roses till then, erupted its ugly potential menace thereby alerting the society that all is not well and IT security could be a major concern, either due to nasty hit or owing to negligent hitch.
  o As there was no major instance reported, world had some apprehensions about the proportion of the problem; some even felt that there was some ground to raise finger to the IT profession.

B) 911 – This nickname, to the subversion that reduced the American skyscraper of World Trade Centre to ashes, has been a landmark on many dimensions like social, international, political, economical, etc. Besides, it was a jolt to the IT as well which was just resurrecting from Y2K. It changed the perspective of the IT Security due to unprecedented scale and shock, underlining the seriousness of the business continuity plan / disaster recovery plan.
4.1.34 Yet another corporate reform that went relatively un-noticed was the surging trends of e-Commerce fueled by the Internet. As they say, Internet years are like dog years; meaning the pace of corporate business was suddenly put in to the next gear and banking was no exception. Due to intense competition necessitating the acceleration in putting through any business transaction, some low priority steps in the workflow got axed down or trivialized. This has a telling effect on security, as some controls started getting diluted, e.g. testing in software development, tallying the balance transfer during migration and manual checking in routine operations, etc.

4.1.35 Along side, there were certain the regulatory directives issued by Reserve Bank of India and guidelines issued by Indian Banks’ Association. Few major ones are listed below:

A) Reserve Bank of India’s Report on Information Systems Audit and IT Security submitted by Dr. Barman Working Group

B) Indian Banks’ Association’s Booklet on Preventive Vigilance in Indian Banks brought out by a study Group under chairpersonship of Mrs. Ranjana Kumar

C) Reserve Bank of India’s Directives on Internet Banking brought out by the committee under chairmanship of Mr. Mittal
4.1.36 Indian banking was responsive to the IT Security implications and many tech-savvy banks have constituted IT Security organization comprising various levels, like directors’ security committee, a separate IT Security section under IT Dept. headed by an executive, etc.

4.1.37 Top rung of some banks have promulgated IT Security Policy, deployed automated IT Security tools, undertaken campaigns to spread IT security literacy, started security audits, etc. In the ensuing chapters an attempt is made to ascertain the need for IT security and related efforts in Indian Banking.
4.2 IT Security

4.2.1 IT Security Scenario

A) Ever since IT was deployed for positive and constructive ends, the frictional forces of IT security quickly set into action dampening the IT effectiveness. It was first time predicted probably by Akio Morito of Sony Corporation in 1986 that information security will become an even bigger problem, as we move into the next century, especially as even the new smaller computers get ability to operate at blinding speed, making millions of computations in seconds.

B) There have been very few people, who seem to be too optimistic, that dare to say, ‘All these security incidents, however, will be minor in the long run’.

C) In the past twenty years this prophecy turned a reality as can be noted from statement made by Ms. Valerie McNiven, Cybercrime Advisor, US Govt. in 2004 narrating the fact that in 2004, the cyber crime overtook Drug traffic by crossing US dollar 100 billion.

D) Even banking segment is no exception to such cyber frauds. The recent statistics by FBI reveals that internet embezzlements are on high rise as follows (figures in US$ million).
E) A quick opinion of such cyber frauds could be easily made that bank customers have certain apprehensions about their bank accounts and operations due to all these negative instances. In one customer survey on Mobile Phone Banking a question – “Are You comfortable with mobile phone banking service?” – was answered with a big “No” by as many as 60% customers stating the explicit reason behind as their security concern!

F) This could be attributed to the twin factors of (a) Growing dependence on the machine and (b) Relatively low maturity of the man. Gone are the days, when IT was just a supporting or staff function; today IT is a backbone of the whole organization in many cases.

4.2.2 To start with, the IT security mishaps are categorized into attacks and accidents. An attack is caused by some deliberate attempt to gain some undue advantage or to bring about a loss to the victim or both, whereas the accident is a result of sheer
ignorance or laxity of the person who operates / gets benefit of IT. In the next few pages three broad points are discussed, viz.

A) Few accidents in the field of IT are narrated and along side the underlying lack of security awareness is shown to emphasize the dire need for security training.

B) So called dichotomy of accidents and attacks is then discussed to demonstrate that such a clear cut dichotomy is not always possible and at times the lines of demarcation are quite obscure and mystical.

C) Finally several real life cases of attacks are duly classified with certain parameters, like magnitude, causal analysis, techniques, etc.

4.2.3 Accidents in the field of IT

Here is an account of some of the noted accidents. Along side, its rationale and rubric is also presented.

A) Date 01.11.2005, Impact – Financial Loss of US$ 10 billion

A computer system failure closed down share trading at the Tokyo Stock Exchange for most of the day, the worst disruption to date for Asia's largest bourse, causing a dollar impact of US Dollar 10 billion.  

B) Year – 1982, Impact – Loss of Human Life

Radiation Therapy device called ‘Therac-25’ of Atomic
Energy of Canadian Ltd. Defects in software used in the device caused massive radiation overdose to as many as 6 patients, killing 4 of them.9

C) Year 1991, Impact – Wrong maneuver of military operations
Patriot missile used by USA in Gulf-war failed because of clock-drift. The effectiveness of the missile dropped from 95% to 13%. The failure was blamed for allowing SCUD missile of enemy to hit American barracks, killing 29 defense personnel and injuring 97 10

D) Year – 1987, Impact – Not so serious loss of time and energy
Researcher recollects a first hand event, where he provided two digits (so to say two boxes) to accommodate the dearness allowance (DA) percentage while designing a payroll system. Later on with spiral trends of inflation, the DA rose to ironically round figure of 100% with a result that computer printed blank spaces in the DA column of pay-slips for all the employees.

E) Year 2005, Impact – Release of criminal due to wrong ID process
Thumb-prints of a suspected criminal J. Brian Jones were wrongly declared by IT of Federal Bureau of Investigation (FBI) as “Mismatch” and hence he was released. 11
4.2.4 As it can be seen, the real cause behind the accidents is the lack of awareness or working skills. At times, anyway, it could be a sheer misfortune with nobody to blame.

4.2.5 Dichotomy of Attacks and Accidents

Generally, it is felt that IT mishaps could be bifurcated into accidents and attacks. By and large that may be the case. However, there are noted instances, where some mishap originates as an accident and is then quickly leveraged into an attack to the advantage of some persons.

A) In the 1930s – the pre-computer era when telephone were quite in vogue – the AT&T Bell Labs operated America-wide network of telephones. Electronics was comparatively not so progressed then and telephone operators used to carry out manual switching to put through the calls. For this drudgery job the Bell Labs used to employ hundreds of school and college dropouts who would engross in rude behaviour with customers, tinkering with instruments, exploring the switching of lines, etc. When one chap accidentally stumbled on a particular frequency of 2600, he noticed that if a long distance call is connected at 2600 frequency, there was somehow no billing in the revenues.
This quickly developed into a huge racket of operators who would offer such long distance calls to the customers at dirt cheap rates. This is a classic example to underline that dichotomy of attacks and accidents is not always possible. Remarkable point to note is that a bulletin was launched after this incident – interestingly titled as ‘2600’ – dedicated to such deceptive IT tricks. Even as of now this happens to be one of the popular magazines amongst hackers with an obvious shift in its medium from paper to website.  

B) Here is another case, where the exact nature as to accident or attack can not be figured out. In a bizarre episode, the pilots of a Malaysian Airlines 777 flying from Perth to Kuala Lumpur had to struggle hard to regain control over aircraft, when it was attempted to be misguided to pitch violently, and then close to stalling.

C) In yet another mystical episode, a data processing problem(?) in the computerized systems at a prison in Michigan, USA has resulted in the early release of some inmates and the prolonged incarceration of others. The cock-up came to light after a state audit revealed errors in
the release date of 23 prisoners between October 2003 and March 2005.  

4.2.6 Security Attacks in IT Arena

As compared to accidents cited above, attacks have marked predominance in terms of count and also the impact. A carefully chosen fifteen examples are given here in a classified manner to help appreciate the astounding characteristics of attacks, like far and wide reach, pinpointed targets, innovative ideas, tremendous monetary loss, humility, anti-sovereign, anti-social aims, out-of-box motives, deep study of applied psychology, and many more.

A) Dormant accounts squeezed by a bank officer

An officer working in a private bank siphoned out funds from inoperative accounts with misuse of a password of her colleague. Such accounts have been known to be a green Pasteur for fraudsters even in manual working era due to lack of customer attention. This fraud was a series of bogus transactions by the bank officer over a period of three years.  

B) Diluted Controls in New Business Practices

With the newer paradigm of business practices, there are
altogether unforeseen types of security attacks appearing on the scene.

Azim Asif, a worker at I-Energizer—a Noida-based call center working for Citibank—came to know personal details of Barbara Campa, a customer of Citibank. Azim created email address for Barbara to order Sony TV worth Rs. 27,000 on 08.05.2002. He was then suspected, nabbed, tried and committed on 05.02.2003 under section 418, 419 & 420 of IPC.

C) Sovereignty of a Nation undermines

India’s Department of Telecommunications (DoT) issued orders to ISPs (Internet Service Providers) in the country to block the URL http://groups.yahoo.com/groups/kynhun, according to a government statement. The URL on the Yahoo Web site was ordered blocked, as it was found to be promoting antinational news, and containing material against the government of India and the state government of Meghalaya, the statement said.

D) Privacy Vs. Office Decorum

Ms. Sharon Smiths installed as the mayor of Houston city in Canada. As a ritual of installation the ceremonial chain, that is an icon of power, was handed over to her by her
predecessor. Later, Ms. Smith and her husband had a photo session with few photographs of her wearing just that chain and no other clothes. These photographs stored in digitized fashion were stolen from the PC and published. While it was a case of individual privacy breach, the public of that city took it as unbecoming to the city and mayoral office.  

E) Simple Thefts of IT Equipments

Researcher had experienced a first hand instance of theft of copper rod used in earthing for himself and seen security incident for few of his clients where paltry IT devices like mouse balls and RAM chips called SIMMs / DIMMs were stolen. All this takes place due to shrinking size of hardware. On a closer web search, it was found that annually survey in US has indicated that as many as 2,08,000 laptops were stolen in a year.  

F) Terrorism

Participation of terrorists in cyber crime was underlined when they reportedly used steganography – a technique of encryption – in their mission of devastating the twin towers of World Trade Centre. There are some security related issues like weather warfare for which there are as many as 20 different patents registered in US.
G) Sophistication

With high degree of micro-processor based sophistication entering daily lives via refrigerators etc. the security has become an issue to bother about, e.g. Distrionic Cruising Systems deployed in modern cars could be hacked and abused to ply the vehicle in a devastating manner. Accidentally, though, yet there is a noted case of how an advanced system in a car manufactured by General Motors has created havoc in US, as the system in that particular car model happened to be in synchronization with the police wireless system.21

H) Physical Injuries

Well-known case ‘Play with Goldfish’ that occurred in America indicates that cyber attacks could result in physical injuries, when small school kids after having enjoyed watching the video clip of goldfish playfully swimming ordered for it and got their finger bitten by piranha that were delivered due to horrendous change of word goldfish to piranha by a disgruntled employee in that company dealing with fish.

I) ID Theft

Identity theft has been a serious crime on rising scale. In Phoenix, the thief has stolen selectively those disks of

J) Confluence of IT with Social Sciences

Applied Psychology and its in-depth utilization has been utilized for cyber crimes. Criminals have been trained in an intensive manner to learn and master the psychological traits of their marks and to influence them to commit the wrong actions of revealing passwords, etc.  

K) Money Equivalence

It's not always the money that hackers are looking for. They may prey upon something equivalent to money, too. Austin Perrott, an Australian, ended up with 17.6 million frequent flyer points without ever taking a flight has pleaded guilty to obtaining financial advantage by deception. He used his job as a Singapore Airlines customer services supervisor to exploit a computer system glitch and opened 29 different frequent flyer accounts in which to gather the millions of points - from loyalty programs with Qantas, Singapore Airlines, Thai Airways, Air New Zealand, United Airlines,
American Airlines, British Airways, Cathay Pacific and Finnair - have been valued at as much as US$590,000.24

L) Ugly Issue of Pornography

Hardly a 3 minutes MMS sex clip involving two Delhi Public School students opened a Pandora's box. The clip first circulated among DPS students. Two students sold it to make quick money. It was then sold to a man for Rs 10,000. The man, whose identity has not been revealed, copied it on VCD and sold it to some shopkeepers in Delhi. It was widely circulated over phone network and it reached all over the country and even abroad. It was also copied to a VCD and sold clandestinely in many cities.25

M) Even VIP names abused to impress the victims

Fraudsters impersonate and steal the ID of virtually anybody. Very recently, it was Dr. Kofi Annan, UN Secretary General, whose good name was misused. The email seemingly coming from Dr. Annan reads:

"I, Dr. Kofi Annan, Secretary-General of the United Nations, would like to ask your partnership in reprofiling funds over $250m in excess, the funds would be coming via a string of selected banks in Europe and Asia. The Funds in question were generated by me during the oil for food program in Iraq."
I have been getting scandals/ controversy in this regards, you can read more on the links below ….

You would be paid 5% as your management fee. Please do not write back directly to me via my official email address. All further correspondence should be sent to my private mail box (kofiannan4un@o2.pl). As soon as you indicate your interest I will give further details. Remember to treat this mail and transaction as strictly confidential. I will await your urgent correspondence via my private mail box … – Dr.Kofi Annan.26

N) Big corporate banners are also no exception

At times even large corporations, too, fall prey. For example, AOL was a target of hackers through its customer service representatives who had access to the company's main member database. The hackers targeted employees who had the authority to bump people off their accounts and reset their passwords and had access to personal and billing information. Hackers were able to illegally break into 200 of AOL’s member accounts by targeting key company employees with an e-mail virus.27

O) Insiders’ Attack is not an unheard news

Company’s own employees are involved in many attacks
against it; Statistics published year after year by various research groups of world repute point out that behind two out of three attacks there is a hand of insiders. FBI’s Richard Hansen working in the Communication Software Team of Counter-Intelligence Squad was found to have conducted inside attack for more than 15 years. What trojans he planted in software & where all it replicated remains still a puzzle. Instead of merely continuing with such episodes (few listed here just as example), it will be in the fitness of things to move ahead and trace quantitative and qualitative causes related to such cyber crimes.

4.2.7 Relative proportions of the attacks by their types could be interestingly found in the following chart that signifies percentages of victim companies.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>1999</th>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Net Abuse</td>
<td>98</td>
<td>80</td>
<td>92</td>
<td>78</td>
<td>80</td>
<td>60</td>
<td>48</td>
</tr>
<tr>
<td>Virus Menace</td>
<td>90</td>
<td>85</td>
<td>94</td>
<td>85</td>
<td>83</td>
<td>78</td>
<td>73</td>
</tr>
<tr>
<td>Laptop / Mobile Theft</td>
<td>69</td>
<td>60</td>
<td>63</td>
<td>54</td>
<td>58</td>
<td>50</td>
<td>48</td>
</tr>
<tr>
<td>Unauth Info. Access</td>
<td>57</td>
<td>70</td>
<td>48</td>
<td>38</td>
<td>44</td>
<td>37</td>
<td>32</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>32</td>
<td>28</td>
<td>36</td>
<td>40</td>
<td>42</td>
<td>38</td>
<td>32</td>
</tr>
</tbody>
</table>

Table 8: Breakup of Cyber Attacks
These findings (Source: Security by CSI & FBI in 2005 – www.gocsi.org) could be viewed in a line chart.

Figure 4: Cyber Attacks during 2005

4.2.8 Another way to appreciate the real significance of such attacks is to note the huge amounts that were lost in the year 2005 by the top 700 corporates world over.  

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Loss in US$ Million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>42.79</td>
</tr>
<tr>
<td>Unauth. Access</td>
<td>31.23</td>
</tr>
<tr>
<td>Information Theft</td>
<td>30.93</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>7.31</td>
</tr>
<tr>
<td>Insider Net Abuse</td>
<td>6.86</td>
</tr>
<tr>
<td>Laptop Theft</td>
<td>4.11</td>
</tr>
</tbody>
</table>
This could also be better understood with the help of the following bar chart.

![Bar Chart: Loss due to Attacks (US$ Million)](chart.png)

**Figure 5**: Loss due to cyber attacks

4.2.9 Causal analysis as to why there have been countless cyber attacks reveals the answer attributable to many stunning points, as under:

A) Fast Spread of Internet

Firstly, it needs to be appreciated that the sheer pace and spread of Internet has been phenomenal. A survey plots the trends showing the period taken by some technologies to populate and reach a figure of 50 million users: Radio took 38 long years before it was listened by 50 million people, PC took 16 years for the same level of penetration, TV spread
that much in 13 years, while the internet has reached the same figure of 5 crore in flat four years.\(^{31}\)

![Years taken by Technologies to reach a spread of 5 crore Users](image)

Figure 6: Years taken by technologies to reach spread of 5 crore

B) Obscure & Invisible Nature

Secondly, the whole nature of IT is essentially a black box, where nothing is visible clearly, unless the things are interpreted for you by some report thrown out by the system. This results in a sort of handicap for anybody dealing with IT. Such lack of transparency has been an issue not merely for security but for efficiency of normal business operations too, as the people can not get the desired information unless the specific report is called for.\(^{32}\)
C) Lack of In-Person Meeting

Coming to qualitative aspects, two parties transacting a business need not (and hardly) come face to face in cyber-world. This leads to a potent reason, as the identification of a person is hard to establish unless sophisticated tools of digital signatures are used. The Internet provides thieves with a cloak of anonymity, so banks have no choice but to do a better job of validating and identifying consumers during an application process. 33

D) Weak / No Trails

For e-business deals there are very weak trails in IT and at times there are almost no trails. This makes it difficult to fix the accountability on the shoulders of the fraudsters. In some cases the fraudsters have chosen cyber café as a launching pad for the attack thereby making the tracing just as difficult as it gets in traditional crimes when the suspects mingle in the crowds at railway station or bus stand to puzzle the sniffer dogs of police.

The scenario is anyway changing, gradually though, as more than 100 hackers were arrested in the year 2004 that seems to be a really creditable accomplishment. 34
E) Trans-national Operations

As the Internet easily transcends the national frontiers, there are news like a hacker sitting in say Philippines breaks into a website of an Indian company having its web server in America. Though the perpetrator achieves his goal sitting in one country, such cases involve trans-border issues. It means that law of multiple nations (and equally multiple investigation agencies also) is involved, should investigation and / or litigation is resorted to.

F) Precise Targeting

Due to the IP address of each computer on the Internet, it is quite possible to mount an attack in a pinpointed manner; e.g. while surfing on the Internet the IP address of the web site is displayed at the status bar on the monitor, which could be used with UNIX commands like TelNet to reach precisely to that server.

It has been demonstrated, as a prank and not as an attack, that not just computers but even a specific printer could be attacked, using the IP address of that printer as recipient of some print requests.

G) No logistics

Interestingly, there is no logistics involved in the cyber
operations, and so also in cyber crimes. Perhaps that is why, the drug lords are swiftly shifting their business line from drug trafficking to cyber crimes. 35

H) Free Software Tools

It is not very difficult to mount a cyber attack, as there have been many software utilities that bundle the technical complexities to offer automated solutions for free. Such nasty tools are floating in umpteen number on the Internet (e.g. 007 to break the passwords, or a website sendfakemail.com for sending bogus mails as the name indicates). This has given rise to a group of hackers called ‘script kiddies’ who are amateurs engaged in simply downloading such tools from web and misusing it, e.g. Anthony Greco (age 18) arrested for sending 1.5 million SPIM (Unsolicited Instant Message) to myspace.com. 36

I) Nasty Hardware Gadgets

Like software utilities, the hardware gadgets are also abundant in supply; e.g. a nasty device called key-logger (that sits between the CPU and a keyboard to record all the keystrokes given on that computer) has been planted for a day or two an later removed to steal all the keystrokes that were later on neatly analysed to figure out passwords, etc.
The number of key loggers unleashed by hackers are on rise, soaring by 65 percent in 2005 as e-criminals rush to steal identities and information.  

J) Outsourcing

Delegating some business functions to an outside agency has been a set practice these days particularly in the wake of core competencies and cost cutting. Where one organization relies on the other diluting the homogeneity of work processes and work culture and at times even the risk assessments are either done superficially or not continued periodically. Interestingly, of late there have been two instances, viz. JP Morgan Chase and Lloyds, where banks have decided to outsource their IT security infrastructure.  

K) Business Process Re-engineering (BPR)

In case of BPR, the processes are made more customer centric and efficient to ensure a shift from departmentalization of the organizational working to a customer centric processes. In an effort to satisfy the customers with faster service, some controls might be weakened or even thrown overboard due to wrong assessment or improper priorities.  

L) Hire n Fire Policies

These days, the corporates adopt a policy of hiring the
services of employers, where the professionals are selected with their expertise in the respective functional area as the primary criterion and the personal traits like integrity take a back seat. Besides, the loyalty cannot be built up due to the fact that the professional is not going to stay with the company for his whole career, but would be expected to walk away on completion of the assigned task.

M) Lack of Awareness

The last but not least reasons is that many of the above facets are not at all known to a layman, while some others are just hazily surmised. This lack of awareness is one of the prominent reasons why people are increasingly falling prey to cyber attacks. ‘Weak or no passwords’ happens to be a common vulnerability across heterogeneous technological platforms for several years as pointed out by SANS.39

4.2.10 Results of such security attacks could fall in the broad spectrum that starts from paltry or almost no loss and escalate right up to threat to corporate existence including in-between stages of loss of a transaction on hand, loss of customer, loosing the clientele, etc.
A) No Loss

One is fortunate if there is no loss despite some security attack and the attack turns out to be either failure or that the attacker changes his mind due to some contextual matter.

B) Loss of Transaction on Hand

There have been cases of hijacking a session where a particular service and / or deal being tackled in that session is damaged. Other instance is nullifying a specific transaction by hackers who wish to deprive the credit or benefit arising out of it.

C) Loss of a Particular Customer

In a more bizarre instance, the customer may be lost by a company, if that specific customer is targeted and is repeatedly facing some hiccups in putting across the deal with the company under question.

D) Loss of Clientele in general

If the attackers persistently mount some attacks like Denial of Service, etc. it is possible that the victim company stands to lose a group of clientele sharing some common parameter used by attackers, e.g. geographic region, business segment, IP address, Internet Service provider, etc.
E) Tarnishing of Corporate Image

If the website of a company is defaced, it amounts to impact the image of the company. The degree of such tarnishing depends on the significance and frequency of the defacing, etc.

F) Loss of Corporate Existence

In some noted extreme cases, the companies have lost their corporate existence due to repeated attacks that have driven away the complete clientele, e.g. An airline company by name Valuejet suffered severe attacks on its web sites that wiped out its existence. (Web Security by Amrit Tiwana)

4.2.11 Tools & Techniques of Hackers and Criminals

Coming to tools & techniques, there have been plethora of techniques used for cyber frauds and the list is ever increasing. What is presented here is a categorized list of illustrative techniques as grouped under a neat rubric at two levels.

A) Use of Small nasty devices

There are several small gadgets invented for the regular usage in the networking environment. These same gadgets have been repeatedly exploited by hackers to their advantage. It will be pertinent to state that these tools are not
to be labeled as good or bad; they are intrinsically neutral. Much depends on the intentions of the one who uses it.

- **Key-logger**

  This device could be inserted between the CPU and keyboard; i.e. the keyboard cable could be terminated into this key-logger and the cable of this key-logger could be inserted in the CPU slot. Once planted, this device would record all the key strokes typed on the keyboard. Basically invented with good motives of audit trail, this is obviously misused by con tricksters in stealing away the secret information like passwords, IP addresses, etc.

- **Skimmer**

  This device could be described in layman's terminology as a card reader designed to read the information on the magnetic strip on the ATM card or credit card that contains some secret data of the account holder. The device is fixed on the ATM booth doors so that entry inside the booth is confined to genuine customers. Fraudsters have used it by placing a loose skimmer inside the booth accompanying a tricking placard to appeal the customers to ‘get one pass of the card to
clean it’. Eventually, the data on magnetic strip of the cards is stolen and accounts of customers were cleaned.

- **Cell Phone**
  
  Usage of this ubiquitous gadget is increasing like a wild fire. Added to it is the wealth of features it comes with, viz. photo snaps, wireless networking capabilities, internet surfing, email downloading, etc. It has helped criminals to carry all these powers with them under the pretext of carrying a phone, anywhere they walk in including at times the secluded and protected areas.

- **USB Pen Drives**
  
  This is a nice example of how the shrinking size of IT tools has become a menace for security. This device called pen drive – takes it name from its appearance similar to a small writing pen – could be mounted on USB port (a socket on the CPU box to put it simple) and then could be used for data storage having capabilities of reading and writing, to and from the hard disk of the computers. It is therefore very easy for anybody to copy the data on his pen-drive and walk
away easily even through the normal frisking, unless the rigorous measure like strip search are applied.

- Lebanese Loop

This is the height of creative genius of criminals used in destructive manner. A simple plastic sleeve with one end sealed – that appears like a small carry bag – is inserted in the ATM card reader by criminals and its remains outside are neatly cut and pasted so that is can not be easily spotted. After this careful craftwork, the criminal stalk around the ATM booth for his prey. When a customer walks in the booth and inserts his card, the reading operations are not neatly done due to this sleeve resulting in ATM rejecting the withdrawal. The desperate customer has to leave finally without getting his card that is stuck in the sleeve. After few minutes the same criminal walks in again to steal the card by removing the sleeve with scissors and screwdriver. As the trick was a innovation by a Lebanese person, the name Lebanese loop has stuck to it.

B) Software Manipulations

Software as everybody knows is the real power behind the
glory of IT. The best description of software comes from Edward Yourdon, who has aptly described it as ‘executable knowledge’. Since software is the core power to transform & process the data, no wonder it has been exploited by hackers.

- **Trap Doors**

  It is possible for a software designer to deliberately plant some nasty logic in the programs, with which he could gain the control of the system down the line when it is getting implemented. Its ancient analogy could be found in the secret exit door planned in the palace that would be used by king to flee away in emergency situation. Few tales provide an account of how the king’s architect has misused it to gain access to the palace by thwarting the whole security for insurrection.

- **Salami**

  It could be best appreciated as a leaking bucket fraud. Here, the fraudsters manage to siphon out a small sum in each transaction that is generally difficult to sense. With high volume it becomes a substantial gain for them. The noted Zygler case of salami technique in UK tells us how the programmer misappropriated the paltry
amount discarded in the process of rounding of interest for each customer.

- **Buffer Overruns**
  The case of buffer overrun occurs when the input data is more in its size or width or length as compared to the field that receives and stores it temporarily. If the software treats such an error diligently things proceed ahead smoothly. Anyway, if it is a deliberate attempt to overpower the system and software does not check the bounds, then the buffer overflow attacks could help the hacker to gain the control of the full system.

- **SQL Injections**
  The modern applications are powered by some DBMS product or other and all these DBMS software share one common tool called Structured Query Language (SQL). One of the advantages among others is that ordinary users could run SQL commands without much of technical knowledge. It is a set practice of software developers to extend a helping hand to such users by providing the often-required portions of SQL commands ready-for-use, so that users could take this half-cooked command ahead to fill up the requisite
details based on run time requirements. There are some techniques with which the SQL commands may be injected with deadly verbs and words of SQL to make it spill out the data that would have been otherwise tightly guarded for outputs.

- Malicious changes in Parameter Settings

Cyber crimes related to software may not be perpetrated by developers alone. Almost all the software products provide a set of parameters, i.e. the user definable values that would fine tune the application to the specific requirements of the users. There are many examples where the settings of these parameters have been temporarily twisted by ill elements to their advantage.

C) Web Operations

In the past couple of decades, the world wide web (WWW) has become truly all-pervasive. Because of massive spread of e-commerce, the web has been a cynosure of criminals in several ways. Broadly the web services could be classified under following few categories. The tools and techniques under individual category needs some discussion that is done in the next section.
• Email

Email is the single largest application of the Internet. Ever since the hotmail was popularized by Sabir Bhatia, the penetration and reach of email has been galloping. There have been quite a few email defrauding tools like spoofing, phishing, etc. that are narrated in the immediate next section.

• Web Surfing (HTTP)

This is typical net surfing with which one gets the information in the desired area by hunting with the help of search engines like google, mosaic, etc. The techniques like Cross Site Scripting (XSS) are discussed in the next few pages.

• File Transfer (FTP)

The web is also used to transfer the data files from one point to other using what is called a File Transfer Protocol (FTP). Some details on FTP tools are also appended in the next few pages.

D) Email

• Fake Mails

Bogus mails have been a major menace where criminals send bogus mails – playing impostor – to
deceive the recipient who thinks as if the sender was genuine and act upon it. It needs to be noted that sending such con mails is relatively very easy as there is no need for IT expertise and software tools encapsulating all the technological complexities are available on Internet for free download in large numbers.  

**SPAM**

Spam is a trick of sending one and the same mail en-mass to a large population of cyber world. Typically such spam or unsolicited mails are meant for marketing at large and are sent in numbers ranging in millions. These mails clog the network traffic, result in overflow of inbox of people and at times may contain some explanatory files attached to it with an outcome of some other genuine mails getting bounced for want of disk space.

**Phishing**

This attack is relatively of recent origin, where the fraudsters approach their target (again in large numbers running in lakhs) over mail. Posing themselves as officials of some bank, they request the
bank customers to send across their passwords and PINs under the pretext that such passwords have been compromised. Those greenhorn recipients who fall prey and reveal their passwords and PINs may succumb to the later attack when the criminals clean sweep the victim's accounts with the genuine passwords and PINs. Over 50 million PC users are estimated to have received phishing emails which invite them to visit the genuine-looking websites to con them out of their passwords.  

- Emails are also used with all ingenuity just to entice the people. One Mr. Rajprakash Durai of Nagpur, made an appeal in newspaper posing as an agency willing to outsource the email marketing campaign. Candidates were to pay Rs. 3000 as security deposit and then carry on the task of sending mass emails on his behalf, to get Rs. 6,000 at the month-end. The first batch were lucky to get their assurance fulfilled, however, in the second and sizable batch, the culprit eloped after collecting Rs. 3000 per head. It then transpired that it was a nice plot to rob the candidates, where email was used just as a small tool.
E) ID Theft

- Spoofing

Playing an impostor was never so simple till it came to the web. As two persons interacting never come face to face in person, the con trick of impersonation has been widely used in cyber world. Using this trick, the ill elements do rob the people of their social security number, Passport number, credit card number, etc.

- Squatting

Another queer attacks has been used by criminals to exploit the corporate bodies. Here, as a background it is necessary to understand that before a company goes ahead with hosting its website, it has to book the domain name (also called URL name) with the global authority called Internet Assigned Numbers & Addresses (IANA). Thugs booked the various domain names that looks pretty like the name of company and at a later date practically force the company to pay ransom to release their right over that name.

- Credit Card Stealing

When one makes some purchases over the Internet, the credit card of that person has to pass on to the
respective seller, who would claim the payment. Right from keying in the number up to its receipt at other end (including the transmittal in between) the number may be stolen and misused for more such cyber world purchases. This has been nicely worded by Wendy Lehnert when she says, ‘If your credit card number is stored on computer in a text file, you subject yourself to some risk each time you connect to Internet’.

F) Malware

- Virus & Worms

This is the one single attack having the maximum disruptions and financial loss. As indicated in the recent survey, the magnitude of the loss due viruses makes up almost one third of the total financial loss owing to all types of cyber crimes taken together.

It may be stunning to know that with convergence of electronics, telecommunication and computers, the viruses have entered the world of cell phones, too, with varieties like ‘Cabir’, ‘Velsaco’ appearing in 2004 and ‘Locknut’; ‘DamPig’ & ‘ComWar’ in 2005.

- Cookies

Cookies are planted by the web server on the surfer's
computer, when he surfs on the net. These cookies note surfing patterns of individual person and are meant for better and faster service, when the same person hooks up to the same web site on the next occasion, by flashing the data of his choice and preference based on the trends of earlier surfing session. Cookies is a discrete threat to privacy, as they may keep on gathering and classifying the information on the surfing patterns of a person across other sites also (e.g. his financial position as revealed while surfing on bank website, income details noted during visit to government website for filing tax returns, etc.)

• Trojan

The etymological derivation of the term dates back to couple of millenniums when the invincible fort of Troy was overpowered by the building up a colossal hollow wooden horse containing some soldiers inside was kept at the entrance of Trojan fort to entice the people of Troy to drag the horse inside the fort. Essence of the Trojan is a hidden capability and software Trojans have demonstrated such incidences of taking over the control of entire system.
• Spyware

As people started using the web camera for net meetings etc., the hackers have come up with innovative ways of stealing away the animated clips of the victim’s complete movements within their respective rooms. In a worst case, a lady staying in a working women’s hostel fall prey, when the hackers abused her PC and web camera to keep on continually video-shoot all her activities which she was carrying out under assumption that it is completely private enclosure. Later on such clips were sold to the shady dealers in pornography.

G) IT Services

These days the world has seen several IT enabled services like online purchases, information on request, utility services like banking & tax payments, etc. Obviously, the growing usage of such cyber services have invited hackers to impact such services to either their advantage or inconvenience of public.

• Cross Site Scripting (XSS)

XSS is an example where the fake trigger of email is used to lure away the customers in believing that they
are interacting with the genuine organization and not with fraudsters. The mail suggests further interaction like submitting some special information of that customer to that organization by clicking some link provided in that mail. When user does that the link establishes a contact with a dummy website of fraudsters that looks almost exactly like the genuine organization and customers stand to hand over their insider information to these ill elements.

- Denial of Service (DOS)

These days the DOS is interpreted as Denial of Service and not merely as Disk Operating System – the bygone OS. In the DOS attack, the criminals manage to fire millions of bogus requests over web to a specific targeted company, making the network clog and web business transactions with that company are completely down due to this inundation of fake requests. With this, the criminals have completely brought down the web based business of some large companies for a temporary span of few hours.

H) Behavioural
• Shoulder Surfing

It means to note what the person keys in (like password, PIN, etc.) by watching it over his shoulders. This simple trick started playfully by kids to gain computer access to play the games is now graduated by criminals to defraud the ATM customers by stealing away the PIN. The only solution for this could be to be little vigilant when entering crucial information over keyboard.

• Social Engineering

Social engineering is gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is the art of manipulating people into speaking/acting contrary to their normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. They preys on human behaviour, such as the desire to be helpful, the attitude to trust people and the fear of landing in the soup. The real security issue is ultimately the attitude. 46

• Piggy backing

Electronically or mechanically locked doors and
passworded systems are subject to this type of abuse. When it comes to physical piggybacking, the criminal may quickly follow the steps of the genuine user who swipes own card to gain the access. The technique of electronic piggybacking involves the perpetrator intercepting a communication line and substituting their own messages to the legitimate user and/or the system.

- Data Scavenging
  
  Like there have been cases of stealing the secret information of one company by ‘purchasing’ the dustbin contents by rivals, the dumpster diving is possible in electronic way, too. After the execution of a job, information may be left in or around a computer that may be of value. Not only waste paper bins but buffer storage areas of main memory and old data left on discs are all sources of scavenging.

- Foot in Door
  
  This is a starting point for a criminal who wants to mount the attack in numerous steps. He may begin with finding a small loophole in victim’s system to gain an access, e.g. misusing the guest user account that
may not have password. Merely, getting an access with
guest ID does not serve the full purpose as the
privileges attached to that ID may be almost negligible.
However, with this, the criminal gets aboard – that is
why it is called as Foot in door – and then expands his
scope of activities.

I) Hi-tech

- Tempest

Technology offers us this excellence where the
emissions from computer screen could be grabbed
from the distance of several meters and to build up an
identical image in a dynamic mode. Tempest tools
have been used by criminals in a mobile van parked
just outside the utility office like banks that are typically
on ground floor to serve the public.

- Homograph

This is one more addendum to the XSS. The link to the
company provided by the fraudsters in their mails have
generally some trick that makes the web URL in the
link appear almost like the genuine web site address.
Generally, there could be some difference or other that
an intelligent user could notice if he observes it
minutely. Now, the hackers have come up with another trick called homograph, with which the link looks exactly like the genuine web site address. Several companies have their web address in English language (and in Roman script). Hacker resort to the use of another script that is almost similar to the roman script and then assume some name that is identical with the name of the genuine company, with the only difference that one occurrence of say a letter ‘о’ (о for orange) is used in some other script, say Cyrillic. Although the computer works on the background representation, it differentiates between the two, anyway, the Cyrillic ‘о’ and Roman ‘о’ are exactly identical as a pattern or syllable thus making the users unable to even dream of such trick.

- High-Tech ATM Fraud

In a noted ATM attack in Paris the crooks used a gantry of devices. They planted a pin-hole camera in a seemingly a wire hanging over keyboard to note the PIN. They used a skimmer, too, to compromise the ATM card holder’s details stored on the magnetic strip on the card. Then there was an electronic transmission
system to send all the compromised information to the wireless set mounted in the van parked nearby the ATM. Finally, the van also had a portable card printing machine to print the fake card, with which they looted the customer's balance within few minutes. In fact, an interesting revelation tells us that while the bogus card frauds have declined, the customer not present (CNP) frauds are on rise. This is because the ATM provides an unmanned location for fraudsters to reach and stay there for elaborate spadework for their crimes.

4.2.12 Security Solutions

After having seen the causes and effects of the security incidents, it will be proper in sequence to have a look at the security solutions that are widely used all over the world.

A) Physical Access

This category relates to all the solutions with which the physical access to IT installations is controlled. They include both manual as well as automated means like

- Watch & Ward Staff that is stationed at the gate and keeps an eye on every visitor to ensure the genuineness.

- Entry Register which has to be filled up by all the visitors specifying the name, purpose, person visited, etc.
• Visitor's Pass / Identity Cards to be worn on person by visitors while they are on the company's premises.
• A Protocol Officer who escorts the visitor as a matter of courtesy and with a hidden intention of ascertaining that visitor follows the security rules.

B) Logical Access Control

• ID Card that (swipe or proximity type) has to be used to establish the credentials of visitors in front of a computerized entry control system
• Password enabled door locks that would open only when the visitor provides his already registered password.
• Biometric Tools that try to assess the bodily traits like finger prints, palm geometry, retina etc. for identity purpose

C) Encryption

This security measure helps to deliberately garble the data while in storage or in transit, so that even if it is copied or read, not much meaningful significance could be drawn by an interceptor. Whenever required, the right person could decipher the coded text to get back the readable data.

There are numerous ways of encryption; a brief account of just three of them is provided here.
• Steganography

In this technique exploited by criminals but not much used in serious business computing, the data to be kept secret is hidden in any computer file like say a .bmp or .jpeg file containing picture file, etc. by replacing the least significant bits in the file with the bits of the message to be hidden. All this is done with the help of software tool that automates the process in so refined a way that one cannot make out picture contaminated with hidden message. On receipt of such file, the right recipient could always extract the secret message.

• Symmetric Key Encryption

Used for ages – even Julius Caesar resorted to this technique, that is why it has also assumed a name as Caesar Code – this method simply replaces each alphabet in the message with some other letter in a formulated manner using some key, e.g. Caesar code uses three as key meaning the word THANKS could be encrypted as WKDQNV by skipping two letters in sequence. At the time of unlocking the message, one has to use the same value (three in this case) as the key to get back the readable message.
• Asymmetric Keys Encryption

Unlike symmetric key method, here the key used for encryption is altogether different than the key to be used for decryption. An extremely complicated scheme based on residual algebra, it is highly popular for digital signatures that are used to curb non-repudiation and to provide legal sanctity to electronic contracts.

D) Public Key Infrastructure (PKI)

This is a well conceived and elaborately developed infrastructure for digital signatures, where the key management is largely handled by specialized agency called certification authority (CA). The role of CAs is monitored by the government authority called Controlled of Certification Agencies (CCA).

E) Firewall

This is an automated tool that safeguards the corporate network from the threats lurking outside, particularly from the Internet that is an open and completely free environment. To keep the risks of attacks from network, the firewall inspects the network traffic is largely in terms of small packets and determines about allowing or rejecting the access to each packet that seeks entry to company’s network, based on the
address of the sender. In addition to this packet filtering firewall, there are other types like proxy server (also called application level gateway) that goes more by semantics rather than just an address. Besides, there is also another type called a stateful inspection firewall which allows only those packets which are received in response to some request going from the company, thereby denying access to those packets which might be sent by an intruder on his own. Lastly, there could be a hybrid variety combining various types enumerated earlier.

F) Authorization

Whatsoever be the degree of high perfection the systems may attain, the role of authorization using manual means cannot be undermined. Hence, there are certain areas like exceptional transactions, system parameters settings, high precision needs and high value deals that are routinely monitored and authorized by human being. In addition to these automated tasks, the authorization has another connotation that suggests manual checking of work done by one human being by another supervisory person. This one-on-one control has been in vogue in many walks by way of testing, audit, inspection, review, etc. Lastly, the word
authorization is at times used in the sense one automated
process ascertains the correctness of the other process put
through in altogether disjoint resources for the purpose of
correctness.

G) Cyber Laws

Assurance is an effective preventive control that provides for
directives for masses as to what they should do and should not do. Coming to IT, there are cyber laws for some of the
nations (like we have Information Technology Act, 2000 that
was enacted on 17 Oct. 2000) that serves as the law of the
land. IT Act provides a legal sanctity to electronic record,
cyber contracts using digital signatures and also defines
various civil and criminal offences with their respective
punitive measures. As pointed out by Shri. N Chandrabau
Naidu, former Chief Minister, Andhra Pradesh, ‘facilitative
legal framework is a sine qua non for the promotion and
development of IT.’  

H) IT Security Policy

For a company, there should be an organizational IT Security
Policy that spells out the DO’s and DON'Ts for its employees.
The policy is quite organization specific relating to its own IT
paradigm and work culture. Like law is to public of the nation,
the policy is to its workforce asserting the management’s security commitment, defining security breaches and providing related disciplinary actions.

Both – the cyber laws and IT security policy – are termed as assurance, as they attempt to provide a reasonable assurance about the IT well-being and prevention of any misuse of computing and communication resources.

I) Proactive Out-of-box Solutions

Over and above the set security solutions that are widely deployed by several companies, there are some innovative and out-of-box solutions to combat specific threats, too. Such security measures are not widely published as they might be proprietary or at times even covert ones. Few such security solutions are described here.

- Safety PIN

To help the ATM customer prevent a forceful attack (where he may be asked to withdraw at gun point, etc.) a creative solution of safety PIN has been brought out with which a customer under duress could indicate his plight to ATM by keying in some other PIN that would be wisely interpreted by ATM software and responded with some phony messages like ‘out of cash’,
‘inadequate balance’, etc. to drive away the thief in despair. 49

- Customer’s Cell phone used for ID & Alert

Some banks have adopted a practice that for any crucial or large credit card / ATM transaction initiated by a customer, the bank may send an automated alert to the customer on his pre-registered cell phone number. Customers’ mobile phones could be thus thought of as ‘Containers’ to load the tokens, as they already have it and carry it all the time. Banks can therefore simply SMS the token code to cell phone of the customer. 50

- Honey Pot

Honey Pot is a deliberately garbled database of a company that is placed on a web server in such a way that it is more susceptible to hackers’ attack. With this, the company has an opportunity to keep a watch on hacking activities to figure out details like place of origin, etc. to nab the criminals. It is quite effective & preferred over earlier approach of simply putting down the attack.
• All security measure not made public

It may be pertinent to note that all such techniques are never brought to daylight for obvious reasons of security. Here are few such examples.

• Reconstruction of shredded documents is now made possible. There have been noted manual means using which during 1979 Iranian people used their exemplary skills of carpet weaving – as many as 400 knots per inch – to recover the documents that were shredded by US Embassy there.

Now, there is similar automated skill set offered by a Houston (USA) based firm, Churchstreet Technology, for reconstruction service for documents that have been conventionally strip-shredded into thin segments. 51

• A Secret capability called ‘Global Identifier’ of MS-Word was successfully used in pinning down David Smith, the creator behind Melissa virus that spread like a wild fire and infected over 1 million PC’s, causing more than $80 million in damage. 52
It is surmised by many experts that highly complex and confidential security measures are used in proprietary way without even seeking patents, etc.

4.2.13 Coming back to set security solutions, various security solutions deployed by the top 700 corporates world over are presented here.\(^\text{53}\)

<table>
<thead>
<tr>
<th>Security Solution</th>
<th>Deployed by %age of Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>97%</td>
</tr>
<tr>
<td>Antivirus Software</td>
<td>96%</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>72%</td>
</tr>
<tr>
<td>Access Control</td>
<td>70%</td>
</tr>
<tr>
<td>Encryption in transit</td>
<td>68%</td>
</tr>
<tr>
<td>User ID &amp; Password</td>
<td>52%</td>
</tr>
<tr>
<td>Encryption in Storage</td>
<td>46%</td>
</tr>
<tr>
<td>Smart Card / Token</td>
<td>42%</td>
</tr>
<tr>
<td>Public Key Infra.</td>
<td>35%</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>35%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>15%</td>
</tr>
</tbody>
</table>

Table 9: World-wide Deployment of IT Security Solutions
This could be better understood with the help of the following bar chart.

Figure 7  (Source: Security survey by CSI & FBI in 2005 – gocsi.org)

4.2.14 Some Popular Misnomers

A) Assumed Safety

People have somehow a queer and preset notion of assumed safety. They feel that software is always flawless, networks cannot be penetrated, default values of settings will protect them, old con tricks don’t re-appear, operating systems and database management systems are quite rugged, known errors are getting patched, etc. Skimming through the past history tells us often that all is not well and there have been so many things goofed up, because of the
well-known saying ‘To err is human’ and human role will never come to an end in the field of IT. There is another dimension to the so called assumed safety that stands on a completely wrong footing, e.g. many bankers feel that the security of passwords of their customers is totally left to the individual customers and bank has neither any propriety nor any reason to educate customers and to enforce secure password practices. These banks think that it is individual who is at risk, but they forget that customers have more access than external hackers and thus could prove to be a potential headache to bank’s security.  

B) Attacks are too difficult

This is another wrong conception in the minds of many people. The matter of fact is that there is a category of hackers called ‘script kiddies’ who thrive on the web with all their mal activities, not because they have high degree of technical expertise, but due to the fact that automated software tools for attacks could be downloaded from the internet and there are umpteen such tools freely available, e.g. password breaking tools, software to send fake mail, etc. It is because of this false sense of security in the minds of people that brings in self complacency about security.
C) It won’t spell a doom

Some have a conjecture that even if attack takes place, it won’t cause a major misfortune. The fact is that there have been several cases in banking, trading, manufacturing and governments where the workforce have burnt their fingers due to catastrophic losses of money, customers, image & existence, too.

D) Security is an Implementation Concern

Yet another segment of population feel that security is botheration to be cared for during implementation only. They feel all that is needed for security is firewalls, encryptions, digital signature, etc. Well, that is never the case. These security measures are just one chunk and other security measures are needed during other walks, viz. software development, network laying, business operations, feeding the input data, handling the printed / on screen reports, etc.

E) Set solutions? First principles!

Security cannot be fulfilled with merely the set solutions. IT is to be thought from first principles. Like earlier mentioned, there is a practice of keeping the password of privileged users in a sealed envelop to make it available to the office,
should the business exigencies demand so due to sudden absence of that person. Due to blind adherence to this, at times people write their password on a small piece of paper and put it without a single fold in a white not-so-thick envelop. Result? The password could be seen without tearing off the envelop by merely holding it against a powerful light. Thus, what is needed is not merely the prescribed solution, but also the action to carry it out with consciously understanding its pro’s and con’s.

F) Event? Process!

Many people feel that security is a one time event, or at the most they look in to it once in a while, as if it were some social function. On the contrary, security has to be viewed as a continuous process that is to be kept on incessantly. Security phenomenon of attacks, accidents, technology, hackers’ tools, etc. keep on continually evolving. It is precisely for this reason that this is viewed as a security continuum.

G) Devices? Human mind!

A noted tendency is observed that workforce feels that security is embedded in gadgets and devices like firewalls, etc. Reality is that security should not end up in gadgets, it
should rather emerge from the human minds that have discretion, creativity and discerning power. But for this, security may degenerate into a mere blindly performed drill or ritual.

H) Secrecy Vs. Openness

There is an eternal debate as to whether security measures should be kept fully secret or they should be thrown open to members of public. It was first brought to limelight when the internal working of locks was published by a priest in eighteenth century.\textsuperscript{55} The crux is that on the one hand the potential fraudsters may learn intricacies about the modus operandi that triggers the rise of crimes, on the other hand the masses need to be educated on this same matter so that they would safeguard themselves. Researcher opines that both the sides have certain validity in their stands and equally any one of this extreme views is harmful if it excludes other completely. It is therefore suggested that neither complete concealing nor en-mass propagation is advisable; instead the knowledge dissemination should address just that subset which is needy of the information. Obviously, in some cases, the whole population – as it is the potential target of attackers – needs to be enlightened
and then the issue remains unanswered as not a problem but rather a reality of life to live with.

I) Automation Vs. Human Intervention

There is also some debate on degree of security automation. Some people feel that security should be automated to the maximum possible degree so that human error and folly will not mar the defense, while other class suggests that automation lacks the discretion that could be provided by human mind only. Here also without tilting towards any sides in a dogmatic manner, researcher suggests that the decision should rather be based on case-to-case merits. Security may not be automated where human mistakes are avoidable with human means, e.g. change of guards, if done at right intervals, helps them to keep alert. In some other cases like securing network from continuous traffic of Internet, the automated solutions are indispensable.

4.2.15 IT Security Principles

A) Defense in Depth

This is an ancient wisdom that says never rely on a single point, as it may turn out to be a single point of failure. This is practiced in IT starting from a simple backup right up to
alternate ways and means for various resources. The concept is also called as onion skill layered security approach. It helps to deter the blended threat with multi-pronged hassles by countering it in a comprehensive way.

B) Minimal Privileges

When one runs a program on a computer, the program assumes the powers and privileges of that concerned user. Hence, the privileges are granted on ‘need to know and need to do’ basis in IT. If it is breached, the super user running a program involving a hidden agenda of virus / Trojan may unknowingly hand over all his powers to the program.

C) No Blind Trust

The maxim suggests that one should never trust the other unless there are adequate established grounds like the long standing and loyalty, correct means of identification, right authorization, etc. It also says that mere repetition does not establish validity. After all, as Mark Buegess tells us, security is about trust and every security problem boils down to a question of whom or what to trust. The same principle has been revealed in the ancient wisdom that says, ‘There is one safeguard known generally to the wise,
which is an advantage and security to all; What is it?

Distrust !!" 58

D) Security Factoring

Here, the security is to be considered as one large entity comprising several small subsets. It is then easier to factor out the small segments and focus on each of them turn by turn to get a thorough feel of the security.

E) Weakest link

Age-old canon of ‘Security of the chain is equal to its weakest link’ points out that the security consists of many components that make up the complete security system and its overall strength is just tantamount to the weakest of the links.

F) Security continuum

Security is never to be treated as a onetime event; It is rather a continuous process where every day there is an inflow of new techniques of cyber crime, novelty devices, innovative solutions, etc. One has therefore to keep abreast with all these in an incessant manner.

G) Check at the gate

It is essential to keep the undesired elements at bay right at the entry point without letting them creep in and later
unknowingly allowing their growth negligently, While some people feel that such matters could be tackled after they become conspicuous and only after they attain a critical size, that is a fallacy. Like cancer is better treated subject to its early detection, same is the truth with all the security issues.

H) Fail Securely

Each system – whether hardware, software, network or combination of all these – has to provide for its own safe and graceful halt, should it fail for some reasons. This is so, because an half-thought and chaotic pause or closure would be cumbersome to manage and may have ripple effects on other surrounding systems.

I) Use well-tried solution

In the matter of security, it is always advisable to deploy a well tried solution. If any measure is not well thought and time tested, there is every chance that it turns out to be faulty and the flaw could result dearly when there are resource demands for other mainstream business purposes.

J) Crosscheck with other channel / means

To ensure the authenticity of a transaction or genuineness
of a message it is a standard practice to check for its origin and correctness with other means / over other channel; e.g. an order placed over telephone is generally confirmed with email and vice versa. This second channel is used with the already registered address / number of the other party to avoid spoofing.

K) Watch the ground for cracks

One has to ensure that the overall working is on a sound footing; that is to say the platforms of hardware, operating system, database management system, etc, should be firm and flawless so that the application stands in a rock solid manner. If this care is not taken the cracks in the foundation may lead to collapse of entire structure.

L) Security is everybody’s duty

One and all in the workforce have to contribute individual role in security – whether it is a sentry or senior manager – to prevent the untoward instances. While the sentry might be entrusted with physical security aspects, the senior manager has to demonstrate visible and vocal commitment to drive the whole workforce on security continuum.

M) Not an Absolute Quantity

Security is a relative term and not an absolute quantity; IT
means that one has to take into account the importance
attached to the assets to be safeguarded, cost of security
measures, discipline and inconvenience it may cause, etc.
and then accordingly plan out the breadth and depth of
security measure to be deployed in that context.

N) Reduce your Attack surface

Each entity or system has some surface that is exposed to
external attacks. Such vulnerability has to be kept minimum
so that the overall risk is reduced to the extent possible.

O) Create / Use secure Defaults

The systems are generally offered in various modes or
settings that help run the same in slightly varying manners.
The users have a general tendency to go by the default
choices – i.e. they prefer to ignore the parameter setting
that could be exercised by them – and rather go by
whatever system. Hence the system should offers the most
secure combination of its default values.

P) Attackers Vs. Defenders

- An attacker may strike at his sweet will at any point in
time, the defender has always to be vigilant in literally
24 X 7 manner. This is sheer due to the proactive role
of hackers and reactive role of security administrators.
This entails that security administrators have to be always alert.

- An attacker may strike on a weak link in the security chain, and that is why the defender has to ensure that all the links in the security chain are having an optimal ruggedness. So, securing almost all the links with maximum possible perfection and leaving a few links loose is never as effective as keeping all the links to a reasonably robust.

- An attacker tinkers and probes for unknown vulnerability and path-breaking unprecedented loopholes, whereas the defender safeguards for known vulnerabilities only. This is also inherent to their respective roles and missions. To overcome this, the security needs to be not just studied but researched too.

- A defender must play by rules staying within the framework of acceptable norms of working. On the contrary, an attacker may play nasty and go to any extreme in breaking the law and ethics, because by his very nature he is all set to play foul. This one has been
quite a serious handicap for ages together for police in their tussle against the thieves.

Q) Business precedes Security

Yet another practicable security proposition is that the business precedes security, i.e. in case security measures try to outweigh or overtake the business operations that will not be feasible. All the security solutions have to be commensurate with the mainstream working and any attempts of over-security may kill the business or security itself. 59

R) Security turned 180 degrees becomes Vulnerability

All merits of IT viz. high speed of processing, huge storage, instantaneous retrieval, precise reach, versatility due to software, omnipresence due to networking are all capable of turning out to be a double sided weapon, when their effectiveness is exploited by criminals and hackers by rotating them for the exactly reverse cause. Even traditional security, it was evinced in the first noted bank robbery in Delhi, when unarmed gangsters walked in to a bank branch and diverting the attention of the sentry by asking what is the time, they swung his gun in 180 degrees. As the bust of the gun thudded on his temple, they looted the bank branch
with the same gun. Thus, the IT deployed by an organization is abused by hackers in many cases to their advantage.

S) Controls beget exposures and exposures beget controls

Like a game of thief and police, the controls and exposures keep on triggering each other in a cyclic unending manner, e.g. one has a gate for his house that just keeps away stray cattle, but not human beings. So, he has to provide for a lock that deters gentleman but not a thief carrying crowbar to thwart the lock. Then he has to think of a night-latch fitted on door from inside. This is an endless game. Moreover, with each control there are some other inherent exposures that have to be tackled with some extra controls and this keeps on and on., e.g. passwords are to be kept utmost secret, but then the office work might be held up for want of a person who is absent from duties. So then there is a scheme of keeping the password of the high privileged users in an envelop. This gives rise to possibility of stealing the password by holding the envelop against the powerful light in some cases, or accidental instances of changing the password on the system but not changing the one kept in envelop, etc.
T) Crack in foundation (Openness $\rightarrow$ Closed),

The world wide web (and for that matter the protocol of TCP / IP, too) was initially designed to provide an infrastructure having capabilities of transmitting all types of computer file like text, spreadsheet, graphs, doodling, etc. This scheme was designed by scientists working at CERN particle physics laboratory and they naturally contemplated web as a completely open and free medium of information transfer, whereas down the line business community found this web as a fantastic medium for commercial dealings. So, while the web was brought about as a fully open and free medium of transfer of data, business community suddenly jumped on to it and wanted to make it as a closed entity with access to be open only for their business partners and employees. This is called as a crack in the foundation necessitating Herculean efforts, gigantic costs and substantial manpower to secure the web.
4.3 Training

4.3.1 The subtle difference between the education and training has been eternally discussed and hence the researcher would initially resolve the issue by preferring the training over education, not only because the audience of learning is the employed class in banks, but also for the theoretical foundations explained below.

4.3.2 Education concerns remembering facts and understanding concepts. It is usually taught in school, although self-study is possible. Training concerns gaining skills and is taught in trade schools or business training sessions. On this backdrop, it is clearly felt that security learning could be best done through a focused training and not merely a conceptual education.

4.3.3 Training seems to be better off as against education in yet another sense. As observed by Dr. John A. Kline, among the three domains of learning (viz. psychomotor or doing, cognitive or thinking, affective or feeling), training emphasizes the psychomotor domain of learning. Training that is done in the cognitive domain is generally at the knowledge level and lower part of the comprehension level. Education, on the other hand, teaches a minimum of psychomotor skills. It concentrates
instead on the cognitive domain, especially the higher cognitive levels, i.e., high comprehension and above.  

4.3.4 First attempts to formally install a training organization date back to 1894 when the training school was installed at National Cash Register Co. (NCR) for its salesmen. Similarly, the first multi-company program was run by Harvard University in 1928 for working managers. 

4.3.5 IT & related Security is a matter more of practice than sheer conceptual discerning for the simple reason that bank workforce has to tackle the security issues while discharging their duties at the desk. Bankers cannot be satisfied with merely notional discussions. In the light of this, IT security could be said to be a topic more of training and less of education.

4.3.6 Coming to training related to IT, there is one school advocating that IT training is an overhead inasmuch as IT that aims to reduce the manual workload demands here some efforts towards its implementation. As IT is increasingly adopted world over, more and more people need to be computer literate. So much so, that even for getting education beyond a certain primary point, one has to learn the IT as an education enabler. This radical paradox could be best described in the words of one
UN report that says, "While education is a great equalizer, technology appears to be a new engine of inequality." 63

4.3.7 Legendary Peter Drucker’s stand on the IT training is worth pondering, as he mentions about the technological hassles in IT that hinder the layman’s path to information in apt words, ‘We need to move from ‘T’ to ‘I’ in IT’.

4.3.8 In the field of IT, a substantial chunk of the cost of overall automation project has to be devoted to training. To put it in words of American Inst. of Certified Public Accountants, ‘Time and cost requirements for training are considerable. Training and implementation represent approximately 70% of the total cost of automation. Hardware and software account for approximately 30%. Too many organizations focus on the hardware and software with little consideration given to the training and implementation time and cost requirements.’

4.3.9 Despite such high cost of IT training for human resources, it is to be understood that human role is absolutely essential in any setup howsoever technologically sound it may be. In the second step it also needs to be appreciated that human errors could cause concern in IT operations in a very big way and at times completely mar the process. No amount of technology can make up for problems with the human conduct, so always consider
your “people policies” pretty thoroughly when making decisions regarding security.  

4.3.10 Visionary leaders appreciate the vital role of training and attach due importance to it. In a series of interviews with CEOs, consulting organization Price Waterhouse has quoted Percy Barnevick, CEO of ABB, supporting the cause of training as saying, ‘Continuous training is not just a catch word, it has become an integral part of our organization with real substance. We have increased our training by a factor of three to four in recent years.’

4.3.11 Bank for International Settlements (BIS) has stated that one of the several information technology risks faced by the banks is the error resulting in improper disclosure of information. Prevention of such errors naturally implies the IT security training to bankers.

4.3.12 Some people go to an extreme by saying that technology meant for automation should be so sophisticated as to completely obviate the need for any human intervention; that would in turn nullify the training need, too. Perhaps they forget that any technology, howsoever, automated definitely requires human being behind it. That is where even the world’s largest
company Microsoft has explicitly mentioned that ‘Technology is not a panacea’. 69

4.3.13 IT Training plays a pivotal role in ensuring smooth implementation of IT projects. Hence, the Control Objectives for Information and related Technology (COBIT) focusing on ‘Delivery and Support’ viz. DS 7 harps on Education & Training to Users. 70

4.3.14 The dire need for IT training has been appreciated even by the general management domain in a pragmatic way, e.g. The latest approach of Balanced Score Card recognizes – under one of its four pillars labeled as ‘Future Orientation’ – the objective of Education & Training of the IT Personnel. 71

4.3.15 IT security training should start right at the top, because even the directors are also in need of such training. To put in straight in the words of Richard Nolan, ‘A lack of board oversight for IT activities is dangerous; It puts the firm at risk in the same way that failing to audit its books would.’ 72

4.3.16 Role of IT security training as a preventive control is unparallel. While underlining this, Jack Welch has stated, ‘The first is tight controls … The second way to prevent crises is with good internal processes, such as rigorous hiring procedures, candid performance reviews and comprehensive training …’ 73
4.3.17 The need for IT training in the banking sector has been acknowledged by the regulator i.e. Reserve Bank of India. It says in one of its directives as under:

"The Board should ensure that the directors are exposed to the latest managerial techniques, technological developments in banks, and financial markets, risk management systems etc. so as to discharge their duties to the best of their abilities." 74

4.3.18 Current rate of bank cyber crimes is not very high in India, but one of the reasons behind it is the lack of awareness of fraudsters, too, to some extent. A citation from a book authored by an ex-banker who express his concern about the frauds and embezzlements that would take a new shape with advent of computers – ‘Indian banks are not paying attention to these [computer frauds] aspects. They have a lot to learn from the experience of other countries.’ 75

4.3.19 Such IT security training is required to be imparted to all rungs of ladder in the banking and also beyond. The outsiders needy of IT security training include the bank’s customers and business partners. It may be unbelievable, yet a good number of service providers do not recognize the neat working of bank credit cards, let alone the associated security needs. In one stunning experiment, it is noted that when a credit card with photo ID of a
lady was used by a man for 25 deals in 4 metropolitan places in India, as many as 21 entries went through successfully without anybody bothering to ask clarification about how a man could use a woman’s credit card.  

4.3.20 Training is needed even to imbibe on the minds of people what is the real risk they run. Sometimes it so happens that companies and individuals are often unaware of security risk or assume that eavesdropping is the only risk. They may be concerned about security but procrastinate about taking action. This has been well stated by Edney and Arbassgh.  

4.3.21 This standpoint is quite endorsed by a recent security survey in UK quoted in the April 2005 issue of the magazine PC Quest that reveals, ‘Early this quarter, the UK govt. released a research showing 68% of large companies were infected by virus in 2003 in spite of the fact that 99% of them were using anti-virus.’  

4.3.22 IT security training has yet another not-so-felt dimension. Insofar as the crimes could be traced to human factor as the key issue and not technology alone, the solution needs to originate from human mind, because this is creative and perceptual thinking, the sort of thinking that computers could not do.  

4.3.23 Banks would be justified in IT security training from a very subtle issue that is brought out by management guru Peter
Drucker by saying, ‘Knowledge workers feel, they are more member of their profession than member of whatever company they work for.’ Such a tendency may result in shift of loyalty from the bank to the professional group including the hackers.

4.3.24 Now we come to some intriguing problems in IT Training in banking sector that are discussed in next few points:

A) Computer literacy in Indian banking workforce at large has been almost negligible about a decade back. There is basically substantial pressure on IT Training systems in banks, due to massive and speedy technology deployment on the one hand and relatively too low IT awareness on the other hand as can be seen from the percentage of PC literate staff at the start of this millennium:

<table>
<thead>
<tr>
<th>Type of Bank</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Pvt. Banks</td>
<td>100%</td>
</tr>
<tr>
<td>Old Pvt. Banks</td>
<td>34%</td>
</tr>
<tr>
<td>PSU Banks</td>
<td>22%</td>
</tr>
</tbody>
</table>

B) Secondly, IT Training is not a onetime event but has to continue in a phased manner. The real secret for success is to build knowledge and skills slowly. ‘Don’t try and learn too much in one go. Don't be afraid to read and reread the sections over again. You will be surprised at how much more you can take in and remember the second time.’
C) As the banks have to depute their staff from their respective branches to the training establishments, they face another problem of relieving and relocation. In many cases, the bank staff finds it difficult to focus on training because of his mental attachment to the prevalent branch working that might have suffered owing to staff shortage. At the training stage, the main concern of the organization should be to remove preoccupation of participants while they are away for training.83

4.3.25 In spite of above said constraints, the IT Security training is absolutely essential. Across various deliberations including the latest HIPAA of US, some points stressed for IT well being are … personnel security, including such activities as supervision of maintenance personnel by a knowledgeable and authorized person, retaining of access authorization records and the training of personnel in proper security procedures / policies.84

4.3.26 Thorough investigation has provided following list of reasons for financial losses caused by abnormal computer incidents

i. Ignorance / Negligence 50%
ii. Dishonesty 15%
iii. Fire / Water Damage 15%
iv. Sabotage by employees 15%
v. Theft/ Damage by outsiders 5%  

4.3.27 Training in IT Security area is essential from one more standpoint that is quite vital. It revolves around the change management in the mindset of people who are not aware of security hassles. A Quote by Andy Grove, Chief of Intel Corp. is worth mention here. “Change can not be managed without changing people which means producing different and appropriate behaviour”  

4.3.28 An ongoing training plan maintains the level of their expertise. When addressing this Sun Tzu asked, "Which side’s warriors and soldiers are better trained?” Quality of on-going training is an important differentiator in information technology. New hacker attacks and techniques crop up every day. In order to deal with these, team must be equipped with knowledge to succeed.  

4.3.29 Security always needs to start at Top. Nearly 2000 computer security experts gathered at SANS conference unanimously point out that top management could better pay attention to 7 Top-Management errors that lead to computer vulnerabilities. They range from ‘Pretend the problem will go away if they ignore it’ to ‘Assign untrained people to maintain security and provide neither training nor time to make it possible to do the job’.  

4.3.30 In the current economic scenario of Liberalization, Globalization and Privatization that is fanned by competition, the bankers have to escalate their customer service to the altitude of customer delight. This puts more pressure and demand on IT trainings. United States General Accounting Office (GAO) Report to Congressional Requesters on Information Security – Technologies to Secure Federal Systems - March 2004 (GAO-04-467) has stated very clearly, "Training is particularly essential if the technology requires personnel to master certain knowledge and skills to securely implement it.”

4.3.31 Issue of IT security training has been underlined in post-911 era with an appeal for more involvement of people in training.

4.3.32 It will not be out of place that training should be proactive and even the organizations that did not ever face any attacks or accidents cannot be self complacent. One of the best ways to get back to basics is through security training. This training should be given annually or to a new employee upon hire. It should educate users on the policies, where to find the policy, and how to implement it. Training should also include reminders on how to identify and report suspicious emails.

4.3.33 The training preparation should start with Pre-Training Survey (PTS) that takes into account all the pro's and con's of the
proposed training before planning out the exercise. Similarly,
after the training program is over, Post Training Feedback (PTF) should also be collected and dwelt upon.

4.3.34 Training may take various forms; One specifically to be thought for IT security is a mock action simulated for hacking attempts. Here, the rigour of US Army could be an instance to follow. US Army has set up a distinct training wing called Opposing Force (OPFOR) – the brigade that trains US troops through mock war exercises. A huge infrastructure by way of large expanse of land with terrains and trenches, artillery, armoured vehicles, etc. has been earmarked for such trials and conditions are kept ever changing to catch the ‘enemy’ unaware. Most important from civil training standpoint is a comprehensive After Action Report (AAR) that takes a detailed stock of the happenings to reap the real benefits of the training. Four essential elements of AAR given to us by OPFOR are worth following:

- Lessons must benefit the teams that extract them
- Lessons must link explicitly to future action
- Leader must hold everyone, himself too, accountable for training
- AAR must start at the beginning of the activity. 92
4.4 **Experience Survey**

4.4.1 The researcher has been an IT Consultant for over a decade; however, the past four years of his practice, i.e. ever since the research was initiated, remarkable experimentation and improvements were brought about in his corporate training practice. Equally, the consulting and training practice also benefited the current research.

4.4.2 In this section the researcher proposes to relate his firsthand experimenting in IT security consulting and teaching / training to examine how this field experience and the current research have impacted and enriched each other. In the process, some account is provided about the researcher’s conjectures that shifted towards conviction in this twin career of research and consulting.

4.4.3 During the past two decades of researcher’s practice, number of banks from all walks have been kindly extending their patronage to his consulting practice. Before starting the deliberations it would be pertinent on the part of researcher to express the gratitude towards these banks and due regards to the workforce that drives these banks.

4.4.4 As stated in one of the earlier chapters, the Indian banking exhibits an intriguing mix of to conflicting features, viz. unity and
diversity, across various dimensions of constitution, business scale, branch spread and sophistication of IT deployment. Each bank has therefore its own specific paradigm and yet the banking sector, in general, indicates an interesting common denominator, too, owing to the same profession.

4.4.5 Researcher has been associated with IT in Indian banking for past two decades and is blessed with a patronage of more than 20+ banks, where he could contribute to IT function of those banks in some way or other. Coming to the particular aspect of IT Security, he has extended his consulting / corporate training mainly to following banks:

• State Bank of India  
  o Largest PSU bank with 9036 branches  
    o 12% Br's under CBS, 88% under TBA  
    o 3612 ATMs plus Internet Banking  
    o Assets of Rs. 4,59,882 Crore  
    o Income 39,547, Net Profit 4,305 Crore  
    o Workforce of 2,07,971

• ICICI Bank  
  o Largest Private bank with 508 branches  
    o Almost all under CBS  
    o 1910 ATMs plus Internet Banking  
    o Assets of Rs. 1,67,659 Crore  
    o Income 12,826 & Net Profit 2,005 Crore
• Bank of India
  o PSU bank with 2551 branches
  o 5% Br’s under CBS, 75% under TBA
  o 260 ATMs plus Internet Banking
  o Assets of Rs. 94,978 Crore
  o Income 7,187 & Net Profit 340 Crore
  o Workforce of 42,500

• Bank of Baroda
  o PSU bank with 2680 branches
  o NIL Br’s under CBS, 83% under TBA
  o 172 ATMs
  o Assets of Rs. 94,664 Crore
  o Income 7,736 & Net Profit 677 Crore
  o Workforce of 39,591

• Corporation Bank
  o PSU bank with 769 branches
  o 43% Br’s under CBS, 57% under TBA
  o 801 ATMs plus Internet Banking
  o Assets of Rs. 33,923 Crore
  o Income 2,815 & Net Profit 402 Crore
  o Workforce of 10,177

• Syndicate Bank
  o PSU bank with 1817 branches
  o Branches under CBS & TBA: 50-50
  o 243 ATMs plus Internet Banking
Assets of Rs. 52,109 Crore
Income 4,323 & Net Profit 403 Crore
Workforce of 26,340

• Bank of Maharashtra
  • PSU bank with 1280 branches
  • No Br’s under CBS, 54% under TBA
  • 45 ATMs
  • Assets of Rs. 32,884 Crore
  • Income 2,753 & Net Profit 178 Crore
  • Workforce of 14,240

• Bank of Rajasthan
  • Private bank with 369 branches
  • 70% Br’s under CBS, 30% under TBA
  • 54 ATMs plus Internet Banking
  • Assets of Rs. 9,154 Crore
  • Income 586 Crore & Net Profit 35 Crore
  • Workforce of 4,070

• Karnataka Bank
  • Private bank with 386 branches
  • 75% Br’s under CBS, 25% under TBA
  • 28 ATMs plus Internet Banking
  • Assets of Rs. 12,526 Crore
  • Income 1,061 & Net Profit 147 Crore
  • Workforce of 4,388

• United Western Bank
  • Private bank with 228 branches
70% Br's under CBS, 30% under TBA
60 ATMs plus Internet Banking
Assets of Rs. 7,083 Crore
Income 552 Crore & Net Loss 98 Crore
Workforce of 3,141

- Cosmos Coop Bank
  - Leading Coop bank with 43 branches
  - All Branches under CBS + few ATMs
  - Other figures indicating business scale & workforce not huge, but IT sophistication is considerably high.

4.4.6 Researcher had an opportunity of interacting in pre-training dialogue with senior management of many of these banks to positively influence their policy decisions on IT security training (in respect of training coverage, methodology, audience, batches etc.) and has carried out the major part of the actually imparting the training as well. This discerning process and the outcome is narrated in the next few sections, as it constitutes the researcher’s major contribution in the field experiment.

4.4.7 The full account provided in the next few sections does not however provide any of the individual bank’s name – though they are from the above listed set – for the obvious reasons of secrecy and professional ethics. Another point to state is that
this account is neither chronological (majority of these activities are performed in the four year span of 2001 – 2005 though) nor is it bank-wise. The approach taken is rather more of a logical rubric.

4.4.8 All the ensuing nuggets were brought out from these banks by the interactive process of

- Brief Talk with Top Brass
  This was more or less focused on synchronization of IT, IT security & Business and the executive concern about funding, organizing, prioritization, motivating and monitoring the training

- Depth Interview with IT Heads
  These meetings threw light on IT paradigm of the Bank that differs from organization to organization; still the common thread among all was a revelation of low IT awareness and even lower IT security awareness among the rank and file. It may look odd, but the IT Heads of some organizations – in almost half the cases – were ignorant about the niceties of IT security, nascent threats and path-breaking recent solutions. They were observed to be banking more on the set notions of security measures.

- Interaction with Training Heads
  These detailed sittings helped to get a closer look at the
training portfolio of the banks. 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 foreign subject to them with an invariable reliance on IT department about not just content and courseware, but also for the training methods, duration, audience, etc.

- Deliberations with officials from IT & IT Security Departments
  During the threadbare sessions with these people at brass tacks, number of interesting issues came to the fore, e.g. dependence of banks on the vendors for security knowledge (not mere products or services), relatively low importance attached to IT security within overall IT portfolio, dominance of compliance as a stand point over the intrinsic hardening of security, lack of or low proportion of security reviews, superstition about branded products and services and lastly above all – the dire need to upgrade their conceptual knowledge and working skills in the arena of IT security.

- Chat with the Branch Officials
  Cursory discussions at bank branches also contributed to the research. This is the grass root level where the public interface and transaction handling takes place. In other words this is the cutting edge, where the IT security impact and awareness
should be clearly palpable. Unfortunately, this class 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.

- Interaction with Participants of Training

Dialogue with 1000+ participants (in 50 programs for 25 banks in past 4 years) was a revealing discussion with a complete cross section of Indian banks that unequivocally underlines the single most important finding of this research, viz. dire need of training inputs for bankers to bring their IT security awareness to an optimal level whereby banks could look forward to have a reasonable assurance that security mishaps would be prevented or detected and corrected.

4.4.9 What is discussed in the next few section is the major vehicle of formal training programs used for all the banks listed at the outset of this chapter.

4.4.10 Audience

- The participants for training programs are segmented as under:
  - Top / Senior Executives from across all functions
  - IT Pro's specializing in Software, Networking, Support
  - Officers from Inspecting, Audit, Vigilance Departments
- Officers looking after Physical security
- Faculty Members at Bank’s Training Colleges

- At hardly a couple of exceptional cases, the bank made it a point to have a mixed audience comprising all rungs of ladder from Inspection, IT & IT Security and Vigilance Departments. This heterogeneity substantially lowered the interaction and marginally reduced the effectiveness and hence was discouraged and discontinued from that time.

- These officials cited above are chosen on priority basis, because they exhibit few significant traits
  - First and foremost in need of IT Security inputs
  - Potential to directly improve the IT Security
  - Capability / Role of spreading security message down the rungs

4.4.11 Coverage

issues, Core Banking Solution and its implications, Internet Banking and concerned care, Futuristic Glimpses of IT Security, etc.

- Like software, these programs are also to be essentially customized by way of considering individual bank specific items like IT spread & sophistication, Business scale and branch network, IT security maturity within the organization and lastly the IT Sec Policy (if established)

- This coverage has been by and large quite effective and acceptable barring few exceptions where some trivial modifications were necessary.

4.4.12 Duration

Length of program ranged between few hours to few days:

- **120-150 minutes** for a fast paced bank having blistering growth for all its staff members including bank’s subsidiary companies

- **Half Day** for Executives like VPs, GMs, etc. to educate them on IT risks in IT Planning, Outsourcing, Monitoring, etc.

- **Weekend Event** One and Half days program for mixed audience from Inspection, Audit, Vigilance
and IT Departments to imbibe preventive and detective IT controls

- **Two days** for IT Officers to provide an elaborate account of IT Security to help them implement it systematically

- **Three Days** Typical Train The Trainers program for members with IT background to enable them conduct similar sessions

- **Five Days** Train The Trainers program for members without IT background to enable them conduct similar sessions

### 4.4.13 Delivery Methods

- **Conceptual Correlation**

  The bankers / participants in the IT security training programs know the IT to some extent and probably the IT related to their daily working very well. Still, they are not in a position to make out the security hassles that are inherent and latent in their IT operations. This is for an obvious reason that they are so groomed to work efficiently within minimum possible time. Their mind therefore takes one simple logical path of a transaction without even having an iota of doubt that various other
permutations and combinations of security breaches are possible within the same transaction.

During the training programs, the trainees are therefore suggested to take stock of their routine chore by standing out of their normal stance and to visualize all odds that could occur per chance or could deliberately be maneuvered by ill elements. It is only when they are suggested to modify their outlook in this way that they start appreciating the real security concerns.

Once they are initiated on such a path, it is easier for them to carry on that progressive march on security continuum on their own, even after the training program is over.

- Introduction to Security Solutions

Second task during the IT security training is to familiarize them with the IT security measures starting from simple solutions like passwords and backup right up to complex ones like digital signatures, etc. The nature and usage of these security gantries takes them one step further in understanding the IT security setup and their significant pro’s and con’s. Wherever feasible, a demonstration is also arranged for them in a PC lab to help concretize the conceptual foundations and grasp the embodiment of the security solution in the systems –
an amalgamation of hardware, software and/or manual procedures. This is done with a total customization for banking domain with a solid bearing on the functional paradigm and also the work culture prevalent in that organization.

Third and final point on the security solutions is probable failures due to their inherent limitations or negligent handling. This takes the participants to the core part of security solutions and instill the mantra that security solutions are to be deployed with all care and a stereo approach might be a complete crash or malfunction.

- **Case Study**

The researcher has accumulated several real life cases from out of his consulting and research, plus the interaction with cyber cell of police that happens to be one of his clients for corporate training on the topic of IT Security.

These cases help participants relate IT security to their every day life, both at bank as well as personal chore by dwelling upon the preventive, detective and corrective controls involved in the cases, as explained below:

(i) Participants get a feel of what a precarious situation one might land into when the exercise suggests them to stand in the shoes of the victim.
(ii) In some other cases, participants are urged to solve the case by working on their detective skills in a logical manner and also to set right the things using corrective measures.

(iii) Lastly, they are also advised to figure out as to what went wrong in the case with the preventive controls and to suggest fitting remedies to keep such instance from recurring.

(iv) As these case studies get deeply rooted in the minds, they facilitate in imbibing the security culture within the bank by passing a subtle message that all is well not well unless tight security controls are in place.

(v) In few cases, the litigation among parties and related outcome is also incorporated to illustrate the statutory scenario and the steps the judiciary process may summon. This also underlines that the case law in the cyber regulations is not yet available in large quantum in India, as the IT Act was enacted in circa 2000.

The case based approach in learning has been picked up and sharpened by the researcher during the special
programs he delivered at renowned managements institutes like Indian Institute of Management, that have in turn successfully mastered it from the Harvard Business School, US of world repute.

As an illustration, a couple of cases are reproduced in the annexure to demonstrate the coverage, look and feel.

- Security Snippets

An experiment worth noting is carried out by the researcher by developing some IT security snippets – a miniature version of a case – by culling out and compiling the published security breaches / incidents that prove more effective in such training programs due to following reasons:

(i) The cases are typically a bit longer to be tackled in corporate training programs of short duration. This is particularly applicable to the cases that essentially need to be studied by trainees before hand. The snippets overcome this by curtailing time and distributing them right at the time of session is also possible.

(ii) The snippets are available in large numbers as their scope and expanse is relatively small as compared to the case. This helps participants to focus on just one or two security
issues at a time. Thus snippet is a concise, crisp and sharpened version of a case with more punch in it.

(iii) More number of snippets are possible to be covered in a short while making a program more participative by assigning one snippet each to all the trainees and asking them to dwell on that and present it. Such a one-to-one assignment would be a time-wise luxury with case handling.

Trans-plating the case based approach in IT security from academics / education to business / corporate training has given a sense of fulfillment to the researcher and equally a deep feeling of real fruitful learning to the participants. As an illustration, a couple of cases are reproduced in the annexure to demonstrate the coverage, look and feel.

- Warming up Sessions on IT Security Extrapolation

By its very nature, the IT security is a topic of great creativity that needs to be unleashed so that participants get a first hand conviction that it is a subject to be thought with originality and not merely to be implemented with set run-of-the-mill solutions. With a view to teach them unshackle from their banking specific pre-set notions a quick 10-15 minute exercise is planned at start of each training day that takes them away from
banking into vastly different domain. Couple of such non-bank scenarios have been culled out by researcher based on his consulting assignments performed for non-bank clientele, as under.

(i) IT security for an automated slaughter plant

This scenario tells the participants how it may not be always the monetary transactions and balance that is to be secured but at times it could be altogether different point like timings for the automated operations like de-feathering, etc. and temperature maintenance in the cold storage stocking the boneless meat, etc. that are to be handled in utmost secure way.

(ii) IT security for Oil Exploration & Distribution Outfit

This scenario again takes the bankers in digging oil wells and managing the smooth flow of oil extracted. The security concern here could be safeguarding of the oil wells from terrorist attacks and to ensure smooth functioning of the SCADA system that automates hundreds of pumps and valves in fluid engineering that regulate the transmission and distribution of the fuel.

- Brainstorm Sessions on Debatable Issues in IT Security
At times IT security sessions turn to be quite drudgery. This is more so, when it comes to highly complex and still important topics like digital signatures, particularly in the post lunch when the audience of working white caller people tend to loose their attention.

Hence few brainstorming sessions are planned in the afternoon on eternally debatable issues to make the atmosphere lively, wide awake and more participative.

Such 10-15 minutes sessions are planted to makes them think on some eternally debatable issues of security. Participants are then encouraged to think on their own and polish their logical thinking in security matter. Couple of such topics are, as under.

(i) Man Vs. Machine

The topic ‘Automated security vis-à-vis Manual security’ brings out the best of the two alternatives. Each approach has its plus or minus, e.g. automation is good at speed and consistency, whereas human approach helps to add discretion and creativity.

(ii) Openness Vs. Secrecy of Security Measures

This scenario provokes the participants’ thinking as both the approaches have been advocated by two different schools with justifiable reasons. Openness is supported to
disseminate the knowledge in the society to prevent the mishaps, whereas secrecy is put forth with a view that potential ill elements in the society gain an insight about the crimes that helps them perpetrate such activities.

♦ Games

In the field of general training (and more so in management programs) the games have been used to demonstrate how principles being preached could be brought into practice and to drive home the points being taught, enlivening the otherwise monotonous training routine, etc.

Coming to IT security the researcher surmised that PC games could play a vital role in the training with following roles the games could fulfill

- Heavy Concepts embodied in Lightweight Mode

  A sweetened pill of the dose gains easy acceptability as given to us by medical sciences. So, the intricate concepts could be wrapped in apparently simple games.

- Enliven the security that is inherently a drab topic

  But for a passionate professional, the IT security is quite a dull topic to all others whose mainstream
operation is either banking or IT deployment. Games help in enlivening it.

- Nurturing a sense of belonging for IT security policy
  When security policy is encapsulated in the games, people look at it in a relaxed mood and try to figure out some solution to the complex issues. In the process, they start developing an affinity to the security policy.

- Leveraging human element of curiosity for learning
  Curiosity, anxiety and eagerness are some of the human tendencies that are cashed upon in these games as a natural process of finding out the answer to the real life security issues in banking parlance.

- Recapitulating at the end of the Training Program
  When the games are projected at the end of the 2-3 days IT security training program, they prove a tremendously effective and effortless recapitulation for one and the all, including the trainer should he miss out any point.

- Ability to ‘Think of Worst’
  Going through a security catastrophe is a very rare and learning experience, but not at all an affordable one. Precisely here, the games simulate any scary security
events in the mental realm and help participants to be prepared for it, should it raise its ugly head. This is one of the biggest gain of the games.

In the light of above projected benefits, the researcher went ahead with below mentioned steps to come up with an out-of-box suit of PC games dedicated to the theme of IT Security

- Conceptualization of the game plot
- Streamlining the characters, events & responses
- Providing an element of simulation where possible
- Incorporating a tinge of real life surprises
- Putting in simple hardware & software platform

Two important ingredients were architected in the process of development of the said games:

- Game Engine (GE)
  - It is the set of software programs that embodies core game functionality and administers the game design / plot.
  - GE tackles the job of picking up the case, flashing choices and managing several levels in case of multi-phase game.
  - GE handles various branching / forking, responds to player actions, decides the next course of steps, etc.
Lastly it reflects on player choices by tracking suitability, context & inter-dependencies and allots bonus / penalty.

- Knowledge Base (KB)
  - KB is an artifact of comprehension & wisdom that provides contextual foundation to game.
  - It is a rich collection of several scenario’s, instances & ground principles accumulated after years of practice and deep thinking.
  - Like GE, the KB is also very much proprietary as it embodies the functional domain.
  - GE without KB would be motionless, just like a vehicle without a person who plies it.

A suit of PC Games thus developed has been experimented during IT security training the researcher provided in his own corporate programs as well as some institutional programs at National Institute of Bank Management, National Insurance Academy, Administrative Staff College of India, etc. and the games received a thumping response. Following advantages were observed and narrated by participants:

- Relief from the serious tone of IT security
- Enabling the simulation of security events
- Deep rooting of newly learned security principles
- Ease of learning in spite of extended hours
- Nice recap of Training if the game is run at the end

4.4.14 Courseware

An extensive courseware by way of reading material was provided however, it has been a general observation that majority of the people do not take pains to read it through. One of the probable reasons could be that the topic of IT security is not from the mainstream – neither a banking topic for bankers, nor a core IT topic for technology people. Even the classic books that read like a novel and yet embody the security principles were also found to be not so effective. It is surmised again that the possible cause might be the overall retarding interest of the society in reading that is overtaken pretty fast by other media; anyway, that is not the topic of discussion in the current research.

4.4.15 Miscellaneous Points

- Outreach Programs: In couple of cases the program was conducted as an outreach program with researcher going into the field; In rest of majority cases it was engaged at Bank’s head quarters. It is however observed that in outreach programs (or programs at HO where participants are posted there), the attendance was remarkably high, whereas in those cases, where participants have to travel few hundred miles to reach the training place, the quorum was considerably low.
• Auditorium Mode: Similarly, in all but one cases it was
    conducted in a compact classroom to accommodate 20-30
    participants to facilitate intensive interaction. In the sole
    exception that was conducted in an auditorium, it turned out to
    be more of a one-way dissemination from the speaker.
    Naturally, the auditorium mode is discouraged.

• Program in its own right: Almost all the programs were
    conducted as a distinct event marked with high efficacy while in
    couple of cases it was suffixed to some other event and
    obviously the overall effectiveness slipped due to participants’
    preoccupation and overshadow of that other program.

• Pre training Survey (PTS): It was tried in various cases over
    email wherever time-wise it was feasible. Generally hardly 10
    to 15% of participants responded to PTS and made some
    suggestions before hand about the contents and methods. This
    could be so, probably because it was the first time that many
    banks arranged IT security program with bankers at almost
    ground zero. PTS may be helpful in next batches in future.

4.4.16 Post Training Assessment

    The efficacy of the training programs has been gauged by the
    researcher on two counts of (i) Spreading the security message
    far and wide by the participants and (ii) IT security hardening
across the hardware, software and networking. These two issues are discussed below:

- **Further Spread**

  The programs helped in a mixed manner towards spread of the security message; based on the participants’ role and seniority:

  - **Train The Trainer**  It made maximum perceptible impact as faculty members found immediate application due to their daily duties
  
  - **Subsidiaries, too**  A notable exception of one bank is worth mention, where security sessions were conducted even for the bank’s subsidiary companies
  
  - **Executives**  They are expected to spread it through the vehicle of their field visits; unfortunately, due to their preoccupations and hectic schedules the IT security still takes a back seat.
  
  - **IT Officers**  This segment has made considerable contribution by
Informally telling security tidbit to their colleagues at Br’s while on support calls.

- In several cases, banks are finding it difficult – almost impracticable – to reach out to every single head and heart in the organization. A potent measure of PC games were suggested to some banks, however, it did not pick up beyond a few discussion rounds. There have been a couple of examples where the banks have been giving just a lip-service to the topic and not a single program has been conducted on IT security.

- IT Security Hardening

Researcher has been striving to judge the training efficacy with post-training feedback and such feedback across almost all the programs has unequivocally signified that the program brought about substantial increase in their security awareness and that they found extensive applicability of the inputs in their daily chore. In some of the programs, the participants have even expressed that it was the best ever training program they have attended so far in their 20-30 years of career and pledged to implement the principles and practices in their days to come.