Chapter 5. Primary Data Collection

This chapter introduces the primary data collection methods of questionnaire and structured / depth interviews. It then moves ahead with the quantitative techniques of tables, factors, clusters, frequency distribution, etc. that researcher has used to analyze this data. Actual results of these analyses are provided in the next chapter.
5.1 An initial set of questions was first drawn up with several questions relevant to IT security in the banking domain. This first questionnaire had break-up of questions as under:

<table>
<thead>
<tr>
<th>IT Security Area to be surveyed</th>
<th>Count of Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Basics</td>
<td>5</td>
</tr>
<tr>
<td>Institutional Issues</td>
<td>3</td>
</tr>
<tr>
<td>Individual Issues</td>
<td>5</td>
</tr>
<tr>
<td>ID &amp; Authentication</td>
<td>9</td>
</tr>
<tr>
<td>Physical Access &amp; Environ.</td>
<td>9</td>
</tr>
<tr>
<td>Logical Security</td>
<td>5</td>
</tr>
<tr>
<td>Data</td>
<td>9</td>
</tr>
<tr>
<td>Software Aspects</td>
<td>8</td>
</tr>
<tr>
<td>Email</td>
<td>8</td>
</tr>
<tr>
<td>Encryption</td>
<td>8</td>
</tr>
<tr>
<td>Networks</td>
<td>9</td>
</tr>
<tr>
<td>Business Continuity Plan</td>
<td>5</td>
</tr>
<tr>
<td>IT Security Training</td>
<td>9</td>
</tr>
</tbody>
</table>

5.2 This draft questionnaire was tested with a small group of bankers at NIBM to find out their views, concerns and suggestions.

5.3 This list having around one hundred items was opined to be too heavy by the group. Although the number may not be that high,
when coupled with the complexity of the very nature of the subject matter, it was appreciated to be a really tough task. Accordingly the draft was trimmed to almost about half of its size and then finalized.

5.4 Modified questionnaires were then used for the subsequent data collection exercise done with the remaining respondents.

5.5 Apart from mailing, respondents were contacted in person, too, at various training outfits like NIBM Pune, ASCI Hyderabad, RBI College, etc. This helped in speedy collection of primary data.

5.6 Besides, the depth interviews were held with some of the top management members from mainstream banking as well as the senior executives leading the IT portfolio. For such interviews the questionnaire was used as a thread, but lot of enlightening deliberations were engaged to exchange the view points. The quantitative aspects of such interviews are presented in the next chapter, while the qualitative aspects emerging in these interviews make up a separate chapter at number seven.

5.7 Following questions have been finally selected for the quantitative analysis that is presented in the next chapter.

- Do you concur with saying ‘IT is a double-sided weapon’?
- Does IT Security need original thinking over & above various gadgets & devices that automate security?
• Does IT Security – assigned to middle management – need any commitment from the top management?

• Is it possible to attain 100% IT security for the corporate computing & communications resources?

• Is IT Security a one-time event, Or is it viewed as a process that is to be continually kept on?

• What is the highest level in your Bank, where the IT Security is discussed on a regular basis?

• Does the bank have a defined & documented IT Security Policy addressing various IT Security issues?

• Is the Policy disseminated / circulated across all rungs of ladder of the bank?

• At what frequency does the bank review and revise the IT Security Policy?

• Is there a mechanism with which bank would come to know about breaches of security policy, if any?

• Does bank have a well-defined IT Security organization with dedicated person(s) within organ structure?

• Is personal safety & privacy recognized within various IT directives & guidelines issued by the Bank?

• Has the bank spelt out any rules related to the password handling?
• Is there any special precaution taken for Laptops carried outside the bank by employees?
• Could the garbage be a source of threat, as it travels from dustbin under the desk to the garbage trucks?
• Do you know about any IT Sec mishap caused due to inadequate/ lax physical access controls in bank?
• Do you understand the risks arising out of viruses, Trojans and worms?
• Do you have the conceptual clarity about the IP Address (Internet Protocol Address)?
• Are there any documented procedures / guidelines about logical access controls?
• If such procedures / guidelines exist, How is their adherence checked by the bank?
• Is the concept of Data ownership documented in IT Security Policy / other procedures of the Bank?
• Do you know what is the Salami technique of a cyber-crime related to banking?
• Have you ever come across a case, where trap doors (also called back doors) were found in software?
• Is the Email account provided by the Bank used for personal purposes also?
• Are there any documented procedures / guidelines about email controls?
• If such procedures / guidelines exist, How is their adherence checked by the bank?
• Are the digital signature used in the bank?
• If digital signatures are used, Is the private key maintained in a secure way by the owner?
• Does the bank use any firewall like proxy server, circuit gateway or stateful inspection?
• Do you know what is the significance of the Denial of Service Attack?
• Please enlist a couple of risks associated with Internet surfing that may be disastrous for bank’s work
• Have you received, read and understood the Bank’s documented Business Continuity Plan (BCP)?
• Have there been any trials to test the effectiveness of the Business Continuity Plan?
• At what frequency does the bank review and revise the Business Continuity Plan?
• Have you received any inputs / training on the implementation of BCP?
Do you know about the concept of ‘Hot Site’ in the Business Continuity Plan?

How frequently is IT Security Training conducted for you / for an employee?

Are the current IT Security training inputs adequate?

5.8 The quantitative data analysis related to above questions by way of frequency distribution, one-point analysis, two factor analysis and three factor analysis is presented in the next chapter.