Chapter 6. Quantitative Analysis

This chapter picks up from the earlier one that dwelt upon the ‘how’ of the analysis. What is presented here is the ‘What’ of the analysis, i.e. the actual findings based on the quantitative techniques, duly supported by numerous tables and also correlation of certain observations that collectively try to throw a new light on the topic.
6.1 The data analysis showing frequency distribution, one-factor analysis & multi-factor analysis and its interpretation is given here, it also provides relevance of the question, the expected answer and its connotation.

- Section 6.2 Brief on constitution of the sample Count 7
  Gives a quick look at the sample of the survey; both in terms of institutions and individuals, i.e. the banks and the officials working there.

- Section 6.3 Simple / One-factor Analysis Count 24
  Presents simple analysis on a single question in a straightforward one per page style.

- Section 6.4 Compound / Multi-factor Analysis Count 6
  Offers multi-factor analyses that cross refer few questions and indicate how response to one query is read in conjunction with few other questions.

- Section 6.5 Segmented Groups Count 14
  Revealing responses to select queries provide interesting responses to some queries put to to some subsets of sample looking after functions e.g. inspection, IS audit, training, etc.
6.2 A quick look is taken here at the sample of the survey; both in terms of the institutions and the individuals, i.e. the banks and the officials working there.

(i) Composition of Banks Surveyed – Constitution-wise

- Public Sector Banks 42%
- Private Banks 28%
- Coop Banks 18%
- Regional Rural Banks 12%

Figure 8: Composition of Banks Surveyed – Constitution-wise
(ii) Composition of Banks Surveyed – IT Sophistication-wise

- High (Total Automation + Interconnectivity) 39%
- Mid (Total Automation at Branch level) 39%
- Low (Partial Automation at Branch level) 22%

Break up of Banks surveyed - IT Sophistication-wise

Figure 9: Composition of Banks Surveyed – IT Sophistication-wise
(iii) Composition of Banks Surveyed – Scale of Business

- High (Assets above INR 1000 Billion) 6%
- Mid (Assets between 100 to 1000 billion) 58%
- Low (Assets below INR 100 billion) 36%

Figure 10: Composition of Banks Surveyed – Scale of Business
(iv) Composition of Banks Surveyed – Branch Network

- High (Above 5000 branches)  3%
- Mid (Between 1000 to 5000)  27%
- Low (Up to 1000 branches)  70%

Figure 11: Composition of Banks Surveyed – Branch Network
(v) Composition of Banks Surveyed – Workforce

- Staff count over 1,00,000  
  4%
- Staff count between 25,000 to 1,00,000  
  6%
- Staff count between 1,000 to 25,000  
  74%
- Staff count below 1,000  
  16%

Figure 12: Composition of Banks Surveyed – Workforce
(vi) Breakup of Respondents – Seniority

Top / Senior Management 11%

Middle Management 19%

Junior Management 70%

Figure 13: Breakup of Respondents – Seniority
(vii) Breakup of Respondents – Functional Roles

IT, IS Audit, eSecurity  37%
Other Functions  63%

Figure 14: Breakup of Respondents – Functional Roles
6.3 The simple data analysis – centered around a single question at a time – showing frequency distribution and its interpretation is given here in next few pages. It also provides relevance of the question, the expected answer and its connotation, for about 25 major questions in the check list.
(i) Do you concur with saying ‘IT is a double-sided weapon’?

Question Rationale

- To find if one appreciates that all IT merits can be reversed to their advantage and detrimental to Bank

Response Received

- Yes 86%
- No 11%
- Don’t know 3%

Interpretation

- As much of 86% of the bankers interviewed are aware of the nature of IT as a double sided weapon, indicating that conceptual understanding is quite clear.

Is IT a double sided weapon?

Figure 15
(ii) Does IT Security need original thinking over & above various gadgets & devices that automate security?

Question Rationale

- To find out respondents impression, if any, that are in favour of security automation beyond reasonable limits

Response Received

- Yes 80%
- No 8%
- Don’t know 12%

Interpretation

- Majority indicate a realization that though IT security is howsoever automated, does need human intervention

Does IT need original thinking over & above security gadgets?

![Figure 16]
(iii) Is it possible to attain 100% IT security for the corporate computing & communications resources?

Question Rationale

- To trace the wrong notion, if any, in the minds of respondents, that absolute security is feasible

Response Received

- Yes 13%
- No 75%
- Don't know 12%

Interpretation

- Majority of respondents are clear that 100% security is an Utopian idea, however some need to appreciate it

Is it possible to attain 100% IT Security?

Figure 17
(iv) Does the bank have a defined & documented IT Security Policy addressing various IT Security issues?

Question Rationale

- To find out whether the banks have articulated their IT security policy for the staff

Response Received

- Yes 60%
- No 22%
- Don't know 18%

Interpretation

- Almost one fourth of the banks surveyed have not yet put in place their IT security policy

Does your Bank have a defined IT Security Policy?

Don't Know 18%
No 22%
Yes 60%

Figure 18
(v) Is the Policy circulated across all rungs of ladder of bank?

Question Rationale

- To figure out the dissemination of the policy

Response Received

- Yes 45%
- No 30%
- Don’t know 25%

Interpretation

- Due to context, response “Don’t know” is tantamount to “No”. Hence in 45% cases the policy is propagated, while it has not percolated in more than half the banks

Is IT security policy disseminated to all rungs?

![Graph showing the dissemination of IT security policy](image)

Figure 19
(vi) Does bank have a well-defined IT Security organization with dedicated person(s) within organ structure?

Question Rationale

- To ascertain whether an organizational chart of the bank has some space for IT security

Response Received

- Yes 68%
- No 12%
- Don't know 20%

Interpretation

- Almost one third of the banks do not have organizational structure for IT security and/or dedicated manpower for that.

Does your Bank have an IT Security Organization?

![Pie chart showing the distribution of responses]

Figure 20
(vii) Has bank spelt out rules related to password handling?

Question Rationale

- To find out whether the most widely obtained control of password is given due importance.

Response Received

- Yes 88%
- No 5%
- Don’t know 7%

Interpretation

- Thumping majority of the banks have taken pains to define and circulate the rules for password – the most primary IT control.

Does the Bank have a defined set of rules for password?

![Bar Chart]

Figure 21
(viii) Is there a special precaution for Laptops carried outside?

Question Rationale

- To assess if the banks are taking proper measures for laptops that are full-fledged computers carried outside

Response Received

- Yes 5%
- No 25%
- Don’t know 70%

Interpretation

- As the laptops are typically taken outside the bank and used by senior executives who handle data critical to top level business decisions, the risk is found to be very high.

Are there any security measures for Laptop carried outside?

![Figure 22]
(ix) Could the garbage be a source of threat, as it travels from dustbin under the desk to the garbage trucks?

Question Rationale

- To ascertain if the workforce knows threats of data theft through the cyber crime technique of dumpster diving

Response Received

- Yes 56%
- No 22%
- Don’t know 22%

Interpretation

- A good proportion of bankers appreciate this risk of data scavenging

Could the garbage be a security threat?

Figure 23
(x) Do you understand the risks arising out of viruses, Trojans and worms?

Question Rationale

 To find out the proportion of bankers aware of the cyber risk of viruses, worms, etc.

Response Received

 Yes 75%
 No 25%

Interpretation

 As many as one fourth of respondents are not aware of this serious risk that has been around for past two decades.

Do you know the menace of virus?

Yes 75%

No 25%

Figure 24
Do you have the conceptual clarity about the IP Address (Internet Protocol Address)?

Question Rationale

- To find out the proportion of bankers aware of internet related IP address and its significance

Response Received

- Yes 57%
- No 43%

Interpretation

- Two out of five bankers seem to be unaware of the IP address concepts used for Internet.

![Bar chart showing responses to the question about clarity of IP Address]

**Figure 25**
(xii) Are there any documented procedures / guidelines about logical access controls?

**Question Rationale**
- To explore the ratio of respondents who have deployed logical access controls in a documented manner

**Response Received**
- Yes 43%
- No 7%
- Don’t know 50%

**Interpretation**
- More than half the workforce is unaware of the logical controls in the bank

Are there documented procedures on logical access?

![Bar Chart](image-url)

Figure 26
(xiii) Is the concept of Data ownership documented in IT Security Policy / other procedures of the Bank?

Question Rationale

- Banks large manpower handles vast amount of data and hence data ownership has to be defined.

Response Received

- Yes 43%
- No 9%
- Don’t know 48%

Interpretation

- Nearly half of respondents indicate that data ownership is clearly defined, while rest are unaware of concept

Is the Data ownership defined in the policy?

Figure 27
Do you know what is Salami technique of a cyber-crime?

Question Rationale

- Salami is a high volume low margin fraud, where a paltry sum is misappropriated for each of the several transactions. It is very typical to financial segment.

Response Received

- Yes 38%
- No 62%

Interpretation

- Almost two third of the banking populace seems to be not aware of this cyber crime technique.

Figure 28
(xv) Have you ever come across a case, where trap doors (also called back doors) were found in software?

Question Rationale

- The trap doors method is used by software developers to plant some hidden software functionality that they could exploit down the lines at implementation phase.

Response Received

- Yes 7%
- No 93%

Interpretation

- Nine out of ten bankers are found to be ignorant of the said cyber fraud technique.

Do you know trap door technique of cyber crime?

![Bar Chart](Figure 29)
(xvi) Is the Email account provided by the Bank used for personal purposes also?

Question Rationale

- Using the office email for personal purpose involves the risk of email spoofing, phishing, cross-scripting, etc.

Response Received

- Yes 30%
- No 52%
- Don't know 18%

Interpretation

- Half of respondents are not clear on the issue, signifying a substantial need for building up awareness

Is bank's email account used for personal purpose?

![Bar Chart]

Figure 30
(xvii) Are there documented procedures about email controls?

Question Rationale

- To find out if the email related procedures exist and at what proportion / scale.

Response Received

- Yes 44%
- No 16%
- Don’t know 40%

Interpretation

- Responses ‘N’ and ‘Don’t know’ are equivalent. There are just two out of five bankers who have email policies in place, indicating large scope for improvement.

Are there rules defined for email operations?

Figure 31
(xviii) Are the digital signature used in the bank?

Question Rationale

- To find out if the banks are using digital signature for entering into cyber contracts that is arriving is a big way

Response Received

- Yes 33%
- No 34%
- Don’t know 33%

Interpretation

- It seems to be an almost perfect trifurcation on the issue, signifying quite a need for building up awareness

Are digital signatures used in the bank?

Figure 32
If digital signatures are used, is the private key maintained in a secure way by the owner?

**Question Rationale**

- To find out whether proper care of the private key (that is crux for the digital signatures) is exercised in banks

**Response Received**

- Yes 33%
- No 2%
- Don't know 65%

**Interpretation**

- Almost two third of the banking populace does not know this facet, indicating need for massive training

**Figure 33**
(xx) Does the bank use any firewall like proxy server, circuit gateway or stateful inspection?

Question Rationale

- To find out general awareness about the firewalls

Response Received

- Yes 50%
- No 8%
- Don’t know 42%

Interpretation

- Half of the bankers are aware of the firewalls, while the rest are divided on conceptual clarity and usage.

Does the bank use firewalls?

Figure 34
Do you know what is the significance of the Denial of Service (DOS) Attack?

Question Rationale
- DOS is a technique where the network is cluttered up with bogus traffic that results into the genuine requests flowing on network getting jammed and thus the service is denied to customers

Response Received
- Yes 34%
- No 66%

Interpretation
- More than half the banking populace is ignorant about DOS attacks that are quite potent for internet banking.

Do you know significance of DOS attack?

Figure 35
Have you received, read and understood the Bank’s documented Business Continuity Plan (BCP)?

Question Rationale

- This question aims at tracing the availability and circulation of the business continuity plan

Response Received

- Yes 24%
- No 76%

Interpretation

- More than three-fourth of the bankers do not know whether the BCP is drafted, let alone knowing the provisions for business continuity

**Did you receive & read bank’s Business Cont. Plan?**

Figure 36
Have there been any trials to test the effectiveness of the Business Continuity Plan?

Question Rationale

- To find out if the regular trials / mock runs are conducted for business continuity plans

Response Received

- Yes 18%
- No 82%

Interpretation

- More than four-fifth of the bankers have not tried and tested the BCP

Were there any trials for BCP?

Figure 37
(xxiv) Have you received any inputs / training on the implementation of BCP?

Question Rationale

- To find out if the training inputs are provided to the bankers on the topic of BCP

Response Received

- Yes 18%
- No 82%

Interpretation

- Four out of five bankers have received no training for the BCP, indicating a serious situation.

Figure 38
6.4 Following are some multi-factor analyses that cross reference some questions and indicate how the response to one question is read in conjunction with few other questions.
(i) IT Security Individual vis-à-vis Institutional Perspective

These tables show how the reasonably good security maturity of individuals dips when it comes to organizational security maturity.

<table>
<thead>
<tr>
<th>Security – Individual Perceptions</th>
<th>Yes</th>
<th>No</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do you concur with saying ‘IT is a double-sided weapon’?</td>
<td>86</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>2. Does IT Security need original thinking over &amp; above gadgets &amp; devices that automate security?</td>
<td>80</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>3. Does IT Security – assigned to middle management – need any commitment from the top management?</td>
<td>76</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>4. Attaining 100% IT security for the corporate computing resources is a myth. Do you agree?</td>
<td>75</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>5. Is IT Security a one-time event, Or is it viewed as a process that is to be continually kept on?</td>
<td>93 (Proc)</td>
<td>7 (Event)</td>
<td></td>
</tr>
</tbody>
</table>

Average Index of Personal Awareness of Security: 82

Table 10: Security – Individual Perceptions

<table>
<thead>
<tr>
<th>Security – Organizational Procedures</th>
<th>Yes</th>
<th>No</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Does the bank have a defined &amp; documented IT Security Policy addressing IT Security issues?</td>
<td>60</td>
<td>22</td>
<td>18</td>
</tr>
<tr>
<td>7. Is Policy disseminated/circulated across all rungs of the organizational ladder?</td>
<td>45</td>
<td>30</td>
<td>25</td>
</tr>
<tr>
<td>8. Is there a mechanism with which bank would come to know about breaches of security policy, if any?</td>
<td>53</td>
<td>7</td>
<td>40</td>
</tr>
<tr>
<td>9. Does bank have Security organization with dedicated person(s) within organ structure?</td>
<td>68</td>
<td>12</td>
<td>20</td>
</tr>
<tr>
<td>10. Is there any special precaution taken for Laptops carried outside the bank by employees?</td>
<td>5</td>
<td>25</td>
<td>70</td>
</tr>
</tbody>
</table>

Average Index of Corporate Awareness of Security: 46

Table 11: Security – Organizational Procedures
(ii) Cyber crime awareness – Generic Vs. Banking specific

This table throws light on the interesting observation as to how the awareness faring as high as 56% on generic cyber crimes is taking a nosedive to 30% when it comes to banking specific cyber crimes.

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Could the garbage be a source of threat, as it travels from dustbin under the desk to the garbage trucks?</td>
<td>56</td>
<td>44</td>
</tr>
<tr>
<td>Do you know what is the significance of the Denial of Service Attack?</td>
<td>34</td>
<td>66</td>
</tr>
<tr>
<td>Do you have the conceptual clarity about the IP Address (Internet Protocol Address)?</td>
<td>57</td>
<td>43</td>
</tr>
<tr>
<td>Do you understand the risks arising out of viruses, Trojans and worms?</td>
<td>75</td>
<td>25</td>
</tr>
<tr>
<td>Awareness Index for Generic IT Security</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>Do you know what is the Salami technique of a cyber-crime related to banking?</td>
<td>38</td>
<td>62</td>
</tr>
<tr>
<td>Please enlist a couple of risks associated with Internet surfing that may be disastrous for bank’s work</td>
<td>42</td>
<td>58</td>
</tr>
<tr>
<td>Have you ever come across a case, where trap doors (also called back doors) were found in software?</td>
<td>7</td>
<td>93</td>
</tr>
<tr>
<td>Do you know about any IT Sec mishap caused due to inadequate/lax physical access controls in bank?</td>
<td>28</td>
<td>72</td>
</tr>
<tr>
<td>Awareness Index for Banking specific IT Security</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

Table 12: Cyber Crime Awareness
(iii) Status of Documented Procedures on IT Security

This table shows that there is substantial scope for streamlining the documentation of the security procedures, as merely half the ground is covered.

<table>
<thead>
<tr>
<th>Documented Procedures on Security</th>
<th>Yes</th>
<th>No</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the bank have a defined &amp; documented IT Security Policy addressing various IT Security issues?</td>
<td>60</td>
<td>22</td>
<td>18</td>
</tr>
<tr>
<td>2. Has the bank spelt out any rules related to the password handling?</td>
<td>88</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3. Are there any documented procedures / guidelines about logical access controls?</td>
<td>43</td>
<td>7</td>
<td>50</td>
</tr>
<tr>
<td>4. Is the concept of Data ownership documented in IT Security Policy / other procedures of the Bank?</td>
<td>43</td>
<td>9</td>
<td>48</td>
</tr>
<tr>
<td>5. Are there any documented procedures / guidelines about email controls?</td>
<td>44</td>
<td>16</td>
<td>40</td>
</tr>
<tr>
<td>6. Have you received, read and understood the Bank’s documented Business Continuity Plan (BCP)?</td>
<td>24</td>
<td>76</td>
<td>0</td>
</tr>
<tr>
<td>Average Index – Documented Security Procedures</td>
<td>51</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 13: Documented Procedures on Security
(iv) Need to strengthen Security Revisions

This table underlines the need for increased frequency in reviewing the security related matters to boost their effectiveness, since the current index is as low as 26%.

<table>
<thead>
<tr>
<th>Frequency of Review of Security Aspects</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is IT Security Policy reviewed / revised at least once in a year by the bank?</td>
<td>24</td>
</tr>
<tr>
<td>2. Is Business Continuity Plan (BCP) reviewed / revised at least once in a year by the bank?</td>
<td>37</td>
</tr>
<tr>
<td>3. Is IT Security training inputs provided to employees at least once in a year?</td>
<td>18</td>
</tr>
<tr>
<td>Average Index of Review / Revision on Security</td>
<td>26</td>
</tr>
</tbody>
</table>

Table 14 : Frequency of Review of Security Aspects
(v) Compliance / Adherence of Security Guidelines

With efforts for compliance looming at below 50%, this table is meant to highlight the dire need for the compliance mechanism for security in the banks.

<table>
<thead>
<tr>
<th>Efforts on Compliance of Security Aspects</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is there a mechanism with which bank would come to know bout breaches of security policy, if any?</td>
<td>53</td>
</tr>
<tr>
<td>2. Is the adherence to procedures on Logical Access controls checked by the bank?</td>
<td>58</td>
</tr>
<tr>
<td>3. Have there been any trials to test the effectiveness of the Business Continuity Plan?</td>
<td>18</td>
</tr>
<tr>
<td>Average Index of Efforts on Compliance Security</td>
<td>43</td>
</tr>
</tbody>
</table>

Table 15: Efforts for Compliance of Security Aspects
Internet Security Appreciation

Depicted in this table is the security appreciation about the ubiquitous Internet that has come to stay as an essential medium for e-Banking.

<table>
<thead>
<tr>
<th>Security Awareness about Internet</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do you have the conceptual clarity about the IP Address (Internet Protocol Address)?</td>
<td>57</td>
</tr>
<tr>
<td>2. Do you know what is the significance of the Denial of Service Attack?</td>
<td>34</td>
</tr>
<tr>
<td>3. Do you know risks associated with Internet surfing that may be disastrous for bank’s work</td>
<td>42</td>
</tr>
<tr>
<td>Average Index of Internet Security Awareness</td>
<td>45</td>
</tr>
</tbody>
</table>

Table 16: Security Awareness about Internet
6.5 In this section, 14 illuminating research observations (one per page) are recorded. These are segmented notings made within a few subset of the overall survey sample of bank workforce, e.g. personnel posted in the functions of (a) training, (b) inspection, (c) IS audit, (d) IT security, (e) physical security etc.

The responses picked up here relate to 2-3 pinpointed questions that are quite relevant and touching some core aspects of these functional segments and the responses and related statistical / graphical ratios underscore the serious void in the understanding exhibited in the concerned functions.
i) A query on Laptop Security to Sr. Executives in Bank

- **Functional Segment**  IT Security – Sr. Executives
- **Question Focus**  Laptop Security
- **Relevance**  Laptops are full-fledged computers that are regularly carried outside the bank, particularly by the senior executives on the move. Laptops are naturally vulnerable to the numerous security attacks ranging from theft of laptop, data leakage as one can read it in public place like airport, data stealing using wireless / infrared mode, etc. These laptops may also be hooked to bank’s network / Internet and then the threat becomes more serious. More aggravating fact is that these senior executives’ laptops have quite potent data. Past surveys indicate that there have been huge laptop thefts – as high as 200,000 p.a.

- **Question**  Is there any special precaution taken for Laptops carried outside the bank by employees?
- **Ideal Answer**  Yes  Ratio of respondents 0 % (zero)
- **Interpretation**  Almost all executives looking after IT security seem to be unaware of this threat.

![Diagram](image)

Figure 39 : Any security measures for Laptops carried outside?
ii) A query on Data Ownership to Sr. Executives in IT Security

- **Functional Segment**  IT Security – Sr. Executives
- **Question Focus**  Data Ownership
- **Relevance**  Large organizations like banks tend to suffer out of the psychological phenomenon called ‘Diffusion of Responsibility’, i.e. what layman calls as everybody’s duty is nobody’s duty. To overcome this, the IT security policy should define the data ownerships, e.g. (i) All the customer accounts data is owned by the respective Branch manager, (ii) Data on investments is owned by the Head of treasury function, etc. In the absence of such definition, an IT-reliant bank may face the problem of accountability.
- **Question**  Is the concept of Data ownership documented in IT Security Policy / other procedures of the Bank?
- **Ideal Answer**  Yes  Proportion of respondents  40%
- **Interpretation**  Majority of the executives seem to be ignorant on this security prescription having bank-wide impact.

![Figure 40: Concept of Data Ownership defined?](image-url)
iii) A query on IT Security Incidents to Sr. Executives in IT Security

- Functional Segment: IT Security – Sr. Executives
- Question Focus: IT Security Incidents / Mishaps
- Relevance: All IT security accidents / attacks have to be recorded on paper or computer, to serve as a single point reference for future. Banks can learn from the past lessons and accordingly improve their security infrastructure and awareness to curb the recurrence. Two reputed surveying organizations in eSecurity, viz. SANS.ORG & CERT.ORG have issued several directives on this issue. ISO 27001 standard also endorses the need for it.
- Question: Do you know about any IT Security mishap caused due to inadequate / lax physical access controls?
- Ideal Answer: Yes  Proportion of respondents 20%
- Interpretation: 4 out of 5 executives in charge of IT security indicate serious void of tracking IT security incidents.

Figure 41: Knowledge / Record of IT security mishaps
iv) A query on Business Continuity Planning (BCP) to Faculty Members

- **Functional Segment**: Faculty Members responsible for training
- **Question Focus**: Business Continuity Planning (BCP)
- **Relevance**: BCP is a pre-thought process that mitigates the impact of any disaster by providing the relevant and commensurate measure to continue the business with minimal disturbance. BCP is recognized as a specific function in its own right in the ever-increasing socio-political menace and BCI.ORG & DRI.ORG have done pioneering work in advancement of BCP. Faculty members are expected to have mastered main sections of the BCP so that they could percolate it down to grass roots.

- **Question**: Have you received any inputs / training on the implementation of Business Continuity Plan (BCP)?

- **Ideal Answer**: Yes  
  Proportion of respondents 20%

- **Interpretation**: A high proportion of trainers lack know-how of BCP that clearly indicates the concerning status of this mission critical task.

![Figure 42: Received any training inputs on BCP?](image-url)
v) A query on IT security training put to Faculty Members

- **Functional Segment**: Faculty Members responsible for training
- **Question Focus**: Training on IT security
- **Relevance**: IT security is a topic as essential (if not more) as any other IT topic. Inputs on this subject are necessary for one and all in the banks, as it has potential to make or mar the IT and in turn the whole bank. Furthermore, in view of the ever-changing milieu of IT security, such training inputs have to be frequently updated and repeatedly delivered to the managers, officers and clerks in the banks. If the faculty members of the bank are not keeping abreast on this, IT security awareness may worsen.

- **Question**: How frequently is IT Security Training conducted for employees?
- **Ideal Answer**: With good frequency of say once a year or more
- **Answer Received**: Just once – 80%, Annual – 20%, More frequent – NIL
- **Interpretation**: Across many a banks, training on IT security awareness is conducted hardly once.

![Figure 43: Frequency of IT security Training](image_url)
vi) A query on nasty small devices put to Physical Security functionary

- Functional Segment: Physical Security role of traditional nature
- Question Focus: Small IT devices having big menace
- Relevance: One of the features of IT advancement is the shrinking size of the devices/gadgets and their increasing capabilities. This has been a headache for IT security as could be seen from a few pocket-sized devices listed below:
  a) Skimmer: Portable card reader, that were used to dupe ATM card holders
  b) Key-logger: Gadget to record keystrokes (theft of Net banking password)
  c) Cell phone: Hi-fi cells have been used for photo-snaps/data transfer

To ward off possibility of intruding such devices rests squarely on shoulders of physical security function manned by retired army/police officers.

- Question: Do you know the nuisance of small gadgets like key-logger, skimmer etc. to bank?
- Ideal Answer: Yes  Proportion of respondents 10%
- Interpretation: Scores of the relevant concerned officials are completely ignorant about these nasty IT devices.

Figure 44: Knowledge of Small Devices & related Nuisance
vii) A query on junction box put to Physical Security functionary

- **Functional Segment**: Physical Security role of traditional nature
- **Question Focus**: Safe-keeping the junction box of Datacomm
- **Relevance**: After having connected all the computers in the bank, the cable is finally handed over to the telecom service providers (like MTNL, BSNL, etc.) who cater banks' Data centers. Junction-box is the device where bank’s cables terminate and the service providers’ cables pick up. A J box is typically put up in some backyard corner unknown to many. Telecom has grown to become an IT backbone for tech-savvy banks and a neglected J box have been an easy spot for criminals to insert their own pair of cables to watch datacomm & spot trends.

- **Question**: Could you show the exact location of junction box (device, in which cables of power/ phone from service provider join cables laid by bank)?

- **Ideal Answer**: Yes

- **Proportion of respondents**: 50%

- **Interpretation**: Half of the security personnel do not even know where exactly the J box is located, let alone the proper care and watch for it.

![Disturbing Facts 50% Ideal Response 50%](image_url)

Figure 45: Location of junction box known?
viii) A query on Business Continuity Plan to Physical Security functionary

- **Functional Segment**: Physical Security role of traditional nature

- **Question Focus**: Business Continuity Plan (BCP)

- **Relevance**: BCP is a pre-thought process that mitigates the impact of any disaster by providing the relevant and commensurate measure to continue the business with minimal disturbance. BCP is recognized as a full-scale function in the ever-increasing socio-political menace and BCI.ORG & DRI.ORG have done pioneering work in advancement of BCP. Security personnel are expected to have mastered the relevant sections of the BCP so that they could help its swift and systematic execution, when needed.

- **Question**: Have you received, read and understood the Bank’s documented Business Continuity Plan (BCP)?

- **Ideal Answer**: Yes  
  Proportion of respondents 10%

- **Interpretation**: A thumping majority of security professionals do not know the BCP issues.

```
Ideal Response
10%

Disturbing Facts 90%
```

Figure 46: Have you received the BCP?
ix) A query on Tracing IT security breaches to Inspectors / Internal Auditors

- Functional Segment: Inspection / Internal Audit
- Question Focus: Tracing IT security breaches, if any
- Relevance: A good IT security policy should be supplemented with a machinery to check its adherence, otherwise the policy remains only in books. This task is to be undertaken by internal auditors / inspecting officers who hop on to various branches for monitoring the controls. It is therefore expected that this workforce should know very well as to how to check the adherence to IT security.
- Question: Is there a mechanism with which the bank would come to know bout the breaches of the security policy, if any?
- Ideal Answer: Yes
- Proportion of respondents: 50%
- Interpretation: Half of the internal auditors / inspecting officers do not know how to look for IT security breaches.

Figure 47: Is there any mechanism to sense IT security breaches?
x) Query on testing weak passwords to Inspectors / Internal Auditors
   • Functional Segment: Inspection / Internal Audit
   • Question Focus: Checking for weak passwords
   • Relevance: A password is marked with following traits:
     a) The most widely used control world-over
     b) Used by even persons at grass root level
     c) Primary control that is often relaxed
     d) Its abuse is the most proximate cause behind many security incidents / frauds

_Passwords have been loosely used en-mass in Indian banking, too, as evinced across umpteen audits._

• Question: Is there any mechanism used to trace out the weak passwords, if any, used by the employees?
• Ideal Answer: Yes   Proportion of respondents 10%
• Interpretation: A high proportion of inspectors / internal auditors lack in expected level of password know-how.

![Figure 48: Is there any mechanism to check weak passwords?](image-url)
xi) A query on IT Security policy definition put to Top Executives

- Functional Segment: Top Executives
- Question Focus: Existence of IT security policy
- Relevance: In the same way as any society needs laws and guidelines to ensure safety and parity, so any organisation requires IT Security Policy to ensure safe use of IT resources.

   It is a document that sets out rules and principles telling all the staff what they should do and should not do with IT.

   A bank not having IT security policy lacks not only formal education on IT security for its employees, but would also find it difficult to treat security breaches, as fixing accountability would be a hard task.

- Question: Does the bank have a defined & documented IT Security Policy addressing various IT Security issues?
- Ideal Answer: Yes  Proportion of respondents  50%
- Interpretation: Half of the top executives say that they do not have security policy in their bank. It clearly is a grave state indicating the fertile ground for IT mishaps.

Figure 49 : Does bank have a defined IT security policy?
xii) A query on awareness of Internet threats put to Top Executives

- **Functional Segment**: Top Executives

- **Question Focus**: Awareness of Internet threats

- **Relevance**: As Internet has become a ubiquitous medium of business, many Indian banks have adopted it to serve their customers. As a flip side of the Internet, many threats like viruses, spyware, data theft, ID theft could be listed as botheration of IT security. Top executives of web-savvy banks are expected to know this facet very well, so that they could check it, lead by example and insist that their juniors take the precautions.

- **Question**: Enlist any two threats arising out of the Internet

- **Ideal Answer**: Most executives should tell about 2 threats

- **Actual Answers**
  - Those who could enlist 2 threats: 5%
  - Those who could enlist 1 threat: 25%
  - Those who could not enlist any threat: 70%

- **Interpretation**: 1 out of four executives could jot down just one threat, while 7 out of 10 are totally ignorant of it.

![Figure 50: Enlist a couple of threats arising out of Internet](image-url)
A query on adherence of logical access put to IS auditors

- Functional Segment: Information Systems (IS) Audit
- Question Focus: Adherence to instructions on Logical access
- Relevance: More than physical access, it is logical access that matters much in IT world. It is administered through used ID, passwords, PINs, biometrics, etc. which decide (a) whether access is to be given to a specific person, & (b) What are the rights / privileges that a person can exercise in his daily chore of operations. Being a subtle control, IS auditors (if not general inspecting officers) are expected to know intricacies of logical access.

- Question: How is the adherence, to the procedures / guidelines of logical access, checked by the bank?
- Ideal Answer: Most of the IS auditors should be able to tell this
- Actual Answers: Those who do not know this aspect at all 60%
- Interpretation: 3 out of 5 IS auditors do not know the logical access and relevant checks they should perform in their audit function.

Figure 51: How is adherence to logical access checked?
xiv) A query on guidelines for Email controls put to IS auditors

- Functional Segment: Information Systems (IS) Audit
- Question Focus: Checking the adherence to Email Controls
- Relevance: Communication service of Email has spread like a wildfire across all continents, including India. The ease, low cost and convenience of the email has a flip side of the ID theft, fooling around victims to get their passwords, PINs etc. It is therefore imperative that banks having deployed emails should enlighten their staff on such risks and keep the threats at bay.

- Question: Are there any documented procedures / guidelines about email controls?
- Ideal Answer: YesProportion of respondents 30%
- Interpretation: As many as 7 out of 10 IS auditors are ignorant about any procedures bank might have put in place for email. It needs hardly any guess as to what could be the status of checking adherence of such procedures.

Figure 52: Are there any documented procedures on Email usage?