Chapter 6

Recent Developments in Banking Technologies:
(Security, Audit and Control-related Aspects)
Chapter 6

Recent Developments in Banking Technologies :
(Security, Audit & Control-related Aspects)

6.1. Introduction

In the area of electronic banking (non Internet-based) in India, we have: EFT and EDI systems initiated by some banks, Off-line and on-line ATMs (Automated Teller Machines, rather, Any Time Money), Shared ATMs (Shared Payment Network System ~ SPNS, called “Swadhan”), Some pilot projects related to the use of Smart-card technology in retail-payment systems (e.g. by Dena Bank), and Use of Internet for marketing and preliminary information services. The world of e-banking (i.e. Internet-banking) is still in its infancy, so there is no way to predict which system will emerge as the favorite. In India, only a few banks have made some beginning on a pilot-basis towards providing preliminary services related to e-banking. So far as other types of organisations are concerned, a large number of “.com” organisations (i.e. virtual organisations) are coming on the scene, and these numbers are increasing every-day at an accelerated rate. Only time to come can tell how many of them will really succeed, sustain and survive in their “.com” business.

The security and other control aspects of some these recent developments occurred during last 3-4 years in the Indian banking industry, are discussed as under.

6.2 Shared Payment Network System (SPNS) - “SWADHAN”

One of the recommendations of the Rangarajan Committee II on Computerization in Banks, 1989, was to set up a Shared ATM Network for banks in Mumbai on a pilot basis to improve banking services. Depending upon its efficacy and cost effectiveness, there is also a plan to replicate this network other major cities.

SWADHAN - SPNS is a large network of ATMs spread over Mumbai, Vashi and Thane connected to a Central Host (refer fig. 6.1 for the schematic diagram). The Banks which participate in this network would issue cards to the customers for transacting on SWADHAN network.
Fig. 6.1: SPNS - Swadhan

- TANDEM/BASE24
- DADR
- AND
- CHEM
- FORT
- DSD
- DSD
- DSD
- DSD
- DSD

Connections:
- 9600 BPS X.25
- ZONE MODEM 3268
- BANK END MODEM 3266
- BSC3270
- A: ATM
- M: MODEM
- AND: ANDHERI ZONE
- CHEM: CHEMBUR ZONE
- DADR: DADAR ZONE
- FORT: FORT ZONE

Leased Line (9.6)
Leased Line
(2.4)Cable Connection
Any customer possessing the SWADHAN-card issued by any member of the SWADHAN-network can go to any ATM linked to SWADHAN, whether situated in the same bank’s branch, or another branch of the same bank or a branch of another bank to do certain banking transactions within the city of Mumbai, Thane and Vashi. The objective behind forming the SWADHAN Network is to provide 24 hours, 365 days/year electronic-banking service to the customers anywhere in these cities through state-of-the-art electronic funds transfer system to be shared by the participating Banks. The SWADHAN project is the first of its kind in India.

6.2.1 Security Aspects of Swadhan

Security is an all-pervasive consideration in SWADHAN – SPNS electronic switching environment. With the growing numbers of the public having access to PCs, Modems, etc., already all the protective features that are available in the ATM industry for securing such a financial-network are provided and supported by the ATMs, the Switch and the Host. The ATM has basically two levels of security: Physical- and Data- Security

6.2.1.1 Physical Security

The Chest is a UL291 rated chest for Business hour or External use. (UL = Underwriter Lab. USA.). This rating is a high when some one tries to drill through. The Chest has thermal-alarm-device which will go off if connected to an Alarm System, when some one tries to weld through. It also can be fitted with a Seismic Device which will go off if some one tries to bang it to open. It also has a Silent Alarm function i.e. if some one uses a gun on a teller and asks him to open the chest, then a different combination of keys will also open the chest....But, it will send a silent alarm to the police station. In this way, there is no blaring alarm that the thief could hear which could endanger the teller’s life. It has a Crook Alarm that will go off if the Chest Door is opened somehow without dialing the correct combination-number. All the Industry standard Alarm system comes with automatic blaring of Alarm if wires to the alarm-system is cut. The output from an ATM to the Alarm system is based on frequency rather than voltage. This means that some crook cannot tap the wires and simulate false conditions to fool the system.

6.2.1.2 Data Security

The data security is implemented by DES- (Data Encryption Standard) –Chip, and information is not stored anywhere after the transaction gets through. Hardware box is also used for full data encryption. The most critical part in regard to the functioning of an ATM is the ATM-Card and the PIN of the customers. As the bank is parting with funds and/or effecting payments from one account to another, based only on the card and the
PIN, sufficient safeguards have to be built into the system to protect the bank from fraudulent attempts. In order to ensure the secrecy of the PIN, encryption methods are used and in a Network all the messages including the PIN have to be encrypted. The PIN is a means of verifying the identity of a customer within an electronic fund transfer system. The objectives of the PIN management is to protect the PIN against unauthorised disclosure, compromise and misuse throughout its lifecycle and in doing so to minimise the risk of fraud occurring within the network. The secrecy of the PIN needs to be assured at all times during the selection, issuance, activation, storage, entry, transmission, validation and deactivation.

The BASE24 supports varying PIN length from 4 - 10. The ISO standard 9564-I recommends a length of 6, same is adopted under SWADHAN PIN type. The customers generally find it easier to remember words using alphabets than just digits. Therefore, under SWADHAN ANSI Alpha Numeric Pin Pads be provided at the ATMs. The Alpha-numeric Pin Pads do not enhance the security, but add to the user friendliness. For example, a customer can remember "SIMPLE" as his PIN, more easily than "746753". Getting observed during the PIN-entry is the most common way that a PIN is compromised. The ATMs should have the PIN pads designed and positioned in such a way that during the PIN-entry, keys are shielded by the customer's body. Where video surveillance systems have been installed, special care should be taken to prevent the possible recording of the PIN by the video cameras. The values of the PIN entered should never be displayed or repeated by audio feedback. The data like PIN, PIN Offset, balance etc., should not be stored in any media at the terminal. Once the customer completes all his transactions, immediately all the data related to his card - PIN, Account number, balance, transaction amount etc., should be totally erased from the memory of the PIN Pad / Terminal immediately and should not be available for anybody, including maintenance personnel entering the ATM. To prevent the ATMs or the responses from the SWITCH being tampered with, the SWITCH and the ATMs should have suitable time limits set for different functions and responses, so that any delay beyond the set limits will result in the customer getting timed out. Under SWADHAN the transaction should be completed between 20 – 25 seconds.

All PIN issuance functions have dual control. The customer comes to the Issuer's location and enters the PIN himself, without disclosing the same to any employee.

Where it is not avoidable, a PIN assigned by an issuer shall be conveyed to the customer by means of a PIN mailer.

71
Validation data is encrypted using PIN-verification key. As the verification is done by the hardware security module in the SPNS, an encrypted PIN verification key is used. The encrypted validation data are in hexadecimal characters. These are converted into decimal numbers using a decimal table which is a random series of 16 digits selected by the user.

After decimalization, the left most digits are taken to form an intermediate PIN. The number of digits is determined by the length of PIN offset. Then the intermediate PIN and PIN offset are added to (using modulo 10 arithmetic) yield PIN check number which is compared with the PIN entered by the customer.

Encryption refers to the process of rendering PINs unintelligible for transmission and decryption refers to subsequently returning PINs to their original form. The whole process includes encrypting, decrypting and translating PINs. During encryption a PIN is presented to the encryption routines in what is called a PIN block. A PIN block is a 16-digit series of hexadecimal characters of which the PIN is a part. The DES algorithm accepts only 16-hexadecimal digit blocks of data for input and hence the PIN block type defines what to do with the gap between the PIN length and DES input requirements.

Maximum PIN tries and other controls are as follows. The maximum Bad PIN tries a customer can make before the system refuses further access to him, should be set in the CAF.

The system, while operating as a transaction-authoriser, provides several types of parameters to control fraud:

- Maximum number and amount of withdrawals can be set at the card and account levels.
- Card and account status indications can be used to flag 'hot' cards. These can be used to capture lost or stolen cards or cards that need to be retained for other reasons.
- The system should be able to operate in either a positive or negative file capacity, basing its authorisation upon the appropriate absence or presence of the account data.

In view of the security risks in transmitting and updating old and new PINs, from ATM terminals, PIN change by the customer should be permitted only at the Issuer bank's system. PIN change should require the current PIN to be entered and verified before the customer is allowed to enter the new PIN, which should be entered twice to validate the
same. The ATM should encrypt both the old PIN and the new PIN when transmitting the data to the SWITCH. Where a PIN is believed to have been compromised, the respective PIN (ATM card) should be deactivated as soon as possible.

a) Key Management
PIN security not only depends upon the encryption algorithms, but also upon sound key management. Keys are an integral part of any security system. In the electronic switching context, keys are inputs to a range of mathematical algorithms and calculations. The algorithms are stored in ‘firmware’ on a hardware device. The keys are stored in the user data area in the hardware device and in the transaction source (i.e. the ATM in the case of SWADHAN). These keys are used to encrypt data / parts of data. The result can be used for various functions like customer identification and verifying message integrity.

i) Security Key Management Procedures
Financial institutions face extremely high risk if their keys are compromised. Thus maintaining the secrecy of keys involved, is of the utmost importance. These should contain the following principles:

➢ keys being secured should be separated into at least two components
➢ each component should be known to only one authorised employee at any point of time and this person should not have access to the other key component
➢ for protection, both key components should be documented, sealed (by a third authorised person) and kept in safe custody
➢ the back up keys should not be stored together

ii) Types of Keys
There are seven types of security keys used in the SWADHAN environment. These are:

Local Master Keys are stored at the Switch. These are in effect the ‘keys to the keys’. That is, they are used to decrypt and interpret all of the other keys used by the system and member banks. The LMKs are extremely confidential and must be accorded the highest form of security available. The prescribed standards for securing the LMKs are outlined as follows. Security for the LMKs will be under the administrative control of IBA. IBA provides a triple-component security procedure. Under this, the LMKs are stored on three different smart-cards, in three separate parts and kept with different personnel for safekeeping.
The following Keys are termed as Member Bank Keys:

PIN Verification Keys (PVKs)
Terminal Master Keys (TMKs)
Terminal Authentication Keys (TAKs)
Zone Component Master Keys (ZCMKs)
Zone PIN Keys (ZPKs)

Member Bank Keys held at the Switch must also be subject to strident security measures.

**Personal Identification Number (PIN) Verification Keys** are used at the Switch to verify the correctness of PIN numbers entered at ATMs. All direct-connect ATMs will have a set of PIN verification keys at the switch. There is one set per member bank. The number of PIN verification keys depends on the type of PIN verification method chosen by the Member Bank. These are the keys used by the Member Banks to issue and verify Customer PINs.

**Zone PIN Keys** are used to encrypt and decrypt information passed between the Switch and member banks’ host computer systems. These keys can be either dynamic or fixed at the time a Member Bank joins the SWADHAN network. When they are dynamic, the Switch will generate these randomly and exchange them with the Member Bank.

**Zone Component Master Keys** are used to generate the Zone PIN Keys. A set of Zone Component Master Keys are needed between the Switch and each Member Bank. These keys are static, and are assigned at the time a Member Bank joins the SWADHAN Network.

**Terminal Master Keys** are used to securely down-line load the Terminal PIN Key from the Switch to the Member Bank’s ATM. One terminal master key is used per Member Bank. These keys are chosen by the Member Bank at the time of joining SWADHAN.

**Terminal Authentication Keys** are used between the Switch and direct connect ATMs. These keys are applied to the Message Authentication Code to verify the authenticity of a message. These keys are chosen by the Member Bank at the time of joining SWADHAN.

**Terminal PIN Keys** are used between the Switch and direct connect ATMs. These keys are dynamically down-line loaded to the ATM by the Switch.
A HSM (Hardware Security Module), a tamper-resistant security module, possesses specialised features and function required for PIN processing. Keys can be either dynamic or static in nature. Only static keys are stored in a Hardware Security Device.

b) Transaction Security
This aspect of security ensures that transactions and messages transmitted across the SWADHAN network are protected from unauthorised decoding and tampering.

i) Message Authentication Code (MAC)
A Message Authentication Code is commonly referred to as a MAC. The process of using a MAC is called MAC'ing. This enables the receiver of a transaction to test for its authenticity, by applying a three-part security algorithm. In SWADHAN MAC'ing is to be used between direct-connect ATMs and the Switch. MAC'ing is compulsory for all new ATMs that are purchased from the date that the first batch of ATMs are certified.

The periodicity of changing of keys will be either 1500 transactions from the terminal or 30 days whichever occurs earlier. The Switch supports PIN / PAN to PIN PAD translation or vice-versa translation.

ii) Hardware Security Device at Switch
The Hardware Security Device located at the Switch contains all of the security keys required for the Switch to communicate with ATMs and host computers. There are two types of keys that are used in PIN encryption between terminals and their BASE24 device handlers. These are transaction keys and master keys. The PINs are encrypted by the terminal using what is known as a transaction key or session key. A transaction key is an encryption-key which BASE24 distributes electronically to its terminals using the same lines over which all of their communications travel. Since transaction keys are distributed to BASE24 terminals using the same lines over which all of their other communications travel, a means of sending transaction keys in a secured manner is required. This security is provided by a separate master key known to both the terminal and BASE24. This master key is used to encrypt transaction keys for their movement over the communications lines. Each terminal's master key must be entered physically at the terminal. The device handlers periodically transmit new transaction keys. If a transaction key load is unsuccessful, device handlers prevent the ATM from opening until a successful transaction key load occurs. The transaction key should be changed at random intervals, at least once for every 50000 transactions at the SWITCH.
c) **Integrity and confidentiality of data flowing on the network**

Message Authentication is a method used to monitor the integrity of data flowing between EFT devices, such as PoS- (Point of Sale) -devices and ATMs and the transaction authoriser. A message can change as the result of tampering or because of communication difficulties. Message authentication identifies whether or not the message has changed. The integrity of the messages flowing in the network is a key to the success of the system. BASE24 supports the generation and verification of message authentication code (MAC) values in Racal - Guardata and Atalla hardware and in software. When message authentication is used, the system sending the message, the terminal or the switch appends a Message Authentication Code (MAC) to the end of the message. The MAC is calculated from the message content and hence it is specific to the message that is created from message authentication coding compiles with ANSIZ9.9.

When the receiving system receives the message, it examines the message content, calculate the MAC and compares it with the transmitted MAC. If the calculated MAC is same as transmitted MAC, the message is accepted for processing, otherwise the message is rejected.

d) **Dynamic Key Management**

The Dynamic Key Management key-exchange service is an optional Visa Service for Members connected to the Single Message System. It enables members to periodically change DEA- (Data Encryption Algorithm) -encryption working keys through the exchange of on-line messages. Because the strength of the encryption process is increased, members are strongly encouraged to use the dynamic key exchange service to support high volume processor to processor connections. Key changes can be initiated in either of the following ways:

- Member sends an administrative request for a new Acquirer and/or Issuer Working Key to Visa. Upon receipt of the request, Visa will generate the appropriate working key and send it on-line to the Member.

- Card Verification Value (CVV) processing is a service that Visa offers to its member banks to counteract the threat of counterfeiting of the cards management stripe. The CVV is a unique check value calculated from the data encoded in the magnetic stripe, using a secure cryptographic process and key known only to the issuer and Visa. Once encoded on the magnetic stripe, the card verification value reduces the threat of
counterfeit transactions by providing for the validation of the cards magnetic stripe information during the authorization process.

c) Password Security

Two levels of password security are addressed. They are: Switch operator password security, and Member bank password security for accessing the Switch.

i) Switch Operator Password Security

As part of their normal duties, Switch personnel will use a normal password to gain system access and perform their activities. To conform with SWADHAN audit and inspection requirements the following standards must be followed:

- To document all occasions on which SUPER password used on the Tandem.
- To list of all instances the SUPER password has been used
- The SUPER password must be known only to senior Switch personnel
- Password has been broken into 3 parts
- Change passwords on a monthly basis

ii) Member Bank Password Security

A separate user-password has been given to individual bank for use when they:

- access the Switch to submit or retrieve files.
- provide ISC with a list of authorised personnel; this would include the photograph and signature of the authorised personnel.
- share their Switch access passwords between only those personnel directly involved with submitting, extracting and maintaining data located at the Switch
- change their Switch access passwords on a monthly basis

f) Logical Data Security at Switch

The customer and account information held at the Switch is the sole property of the member banks. Adequate security measures have been taken to ensure that none of this data is accessible by unauthorised parties. The security standards covering this data are:

- Switch operations or management personnel are not permitted to access customer or account information belonging to member banks in exceptional circumstances like fixing problems and this will be taken on case to case basis.
- All member banks are responsible for securing their data held at the Switch. They are responsible for managing the allocation of passwords and access rights to their data.
- Only member bank staff are permitted to manipulate or alter customer and account information held at the Switch.
- If Switch personnel (including third party technical support staff) require to access customer- and account- data for troubleshooting purposes, they must be accompanied by personnel from the affected member bank(s).

g) Physical Security at Switch

ISC (India Switch Company) is responsible for installing and maintaining physical security measures at the Switch premises.

i) Premises Security

- a close-circuit TV security system is installed with recording facility;
- only authorised personnel are given access to the Switch site;
- an electronic identification access system installed at the Switch site
- no visitors are allowed at the SWITCH site
- a log is maintained for the visitors
- employed armed guard presence at the Switch site;
- security passes are issued to the Switch personnel and visitors;
- there is no non-secured doorways or access-ways to the Switch premises
- a secure and separate area away from Switch equipment and data media are kept for the purposes of:
  - dispatching reports and other media/tapes etc. to member banks or other parties
  - member banks to submit and receive their files to/ from the Switch when they are unable to achieve this from their own sites

ii) Personnel Security Clearance

- all personnel employed irrespective of position are subject to a security investigation to establish:
  - no convictions or substantial allegations against them of financial fraud or impropriety
  - suitable integrity and character to be entrusted with handling highly confidential and sensitive data and information
  - sign a formal non-disclosure agreement, committing that:
    - not divulge to an external party any data or information relating to the Switch’s operation and environment
• not to remove any data or information from the Switch premises relating to member banks accounts
• all operations and systems management personnel are allocated only the system security levels eg. passwords, they require to perform their specific functions
• no personnel of ISC are given access to the Hardware Security Modules containing member banks’ security keys other than exceptional circumstances like fire, flood etc.

iii) Physical Data Security

Procedures to ensure the safe and secure storage of member banks data and information. These procedures should include:

• a process for facilitating the off-site storage of back up copies of member banks’ data
• the provision of a fire-proof and secure space is for the storage of all systems, application and data media both at the Switch premises and off-site storage location
• the secure transportation of back-up data to and from the Switch premises
• the periodic performance of a physical check and audit of all tapes and media to ensure none are missing or unaccounted for
• the maintaining of a media register to monitor the movement of all tapes and other media into and out of the Switch premises

• a member bank’s data does not become mixed with that of another member bank’s
• tapes and other storage media is clearly labeled to minimise the error margin for data from different member banks’ data becoming mixed.
• all hard-copy reports for respective member are clearly labeled and marked so that the prospect of them being distributed to the wrong member is eliminated
• all system reports and information being transmitted to the different member banks is separated to eliminate any prospect of member banks receiving other than their own information

iv) Fire Prevention and Safety Measures At Switch

• the provision of smoke and heat detection alarms
• an abundant supply of fire extinguishing equipment, and appropriate training of personnel in the use of these
**Installation of an appropriate automatic fire extinguishing system**
**a total ban on smoking within the Switch site and its environs**
**fire escape facilities to meet local fire safety regulations**
**regular testing of smoke detectors, fire extinguishing equipment and fire-drill procedures testing of smoke detectors, fire extinguishing equipment and fire drill procedures must be executed at least once a year.**

### 6.2.2 SPNS “Swadhan” Audit Aspects

Within the SPNS environment it is compulsory that there be an audit system in place. This is particularly so given that an independent party (ISC) is responsible for operating the computer infrastructure associated with SPNS.

The financial and accounting aspects of SPNS should also be subject to audit, however these will be mostly the responsibility of individual member banks’ financial auditors.

#### 6.2.2.1 SPNS Audit

The SPNS audit should encompass the following:

- the aspects of the SPNS environment to be audited
- the periodicity of audit
- the party responsible for the audit
- Monitor compliance process

The areas that should be covered during the SPNS audit should include:

- ISC Switch and ATM network operation
- ISC Switch system issues
- ISC Switch and network availability
- Settlement bank to member bank accounting
- Member bank host and ATM availability
- Disbursement of penalty fee funds by SPNS Cell

The following principles may be followed for the various audit categories: The ISC environment should be subject to what is essentially a full and formal EDP/IT-operations audit. This should be conducted in line with standards and procedures used by an external EDP/IT auditor or consultant.
The IT audit of the ISC Switch and network operation should include the following:

- system operation procedures
- network operation and management procedures
- problem management processes (system and network)
- interface procedures between Switch and member bank help-desks / ATM centres
- physical security procedures and measures (i.e. premises security) including fire protection
- personnel security measures
- security of hardware security module containing member bank security keys
- data backup procedures
- off-site storage facilities for backup data
- on-site facilities for data storage
- hardware maintenance procedures
- hardware spares availability
- disaster recovery procedures
- version and change control procedures
- environment maintenance e.g. air conditioning and electrical plant

ISC should develop procedures and processes for each of the preceding issues.

6.2.2.2 Systems Audit

This audit is intended to review the system management procedures and system security aspects of the ISC Switch. The issues covered during this audit should include:

- member bank procedures to submit and retrieve information from Switch
- database recovery
- database integrity
- password control for system operators
- logical separation of member bank data
- end of day processing procedures
- member bank to Switch procedures for card management
- audit trail to be provided
- ensure that all updates to the software are authorised
- ensure that no unauthorised deletions, reversals and alterations to transactions are done to the data during data processing.
- facilitate tracing and reconciliation of disputed data
It is necessary to verify the Switch and network availability statistics being reported by ISC. The audit itself could comprise a relatively straightforward check of daily / weekly / monthly availability-statistics from ISC, compared with corresponding statistics from member banks.

The SPNS Cell will conduct periodic checks of member bank host and ATM availability. The base for this audit will be the availability-statistics collected from member banks and ISC. This can be verified against Electronic Journal etc.

The SPNS Cell should account for the receipt and disbursement of the penalty fee funds received from various quarters. These records should be subject to an independent audit (financial) and should be reported to the SPNS participants.

6.2.2.3 Periodicity of Various Audits
The following table (table 6.1) specifies the periodicity of performing various audits. The SPNS Cell may appoint an IT-Auditor to undertake the following tasks.

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Periodicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC Switch and Network Operations</td>
<td>Six months after SPNS operational inception, and then annually thereafter</td>
</tr>
<tr>
<td>ISC System Audit</td>
<td>Six months after SPNS operational inception, and then annually thereafter</td>
</tr>
<tr>
<td>Switch and Network Availability</td>
<td>Six monthly</td>
</tr>
<tr>
<td>Settlement-Bank to Member-Bank – Accounting</td>
<td>Three monthly</td>
</tr>
<tr>
<td>Member-Bank Host/ATM Availability</td>
<td>Six monthly</td>
</tr>
<tr>
<td>Disbursement of Penalty Fee Funds</td>
<td>Three monthly</td>
</tr>
</tbody>
</table>

6.3 Electronic Clearing Services (ECS)
Electronic Fund Transfer (EFT) facilitates of quick movement of funds from the bank-account of one customer to the bank account of another customer (same bank or another bank in same or different center). Modern world is moving towards EFT while Indian banks are rather slow in this direction mainly because of lack of necessary
communication infrastructure facilities. Once the INFINET becomes fully operational, there will be rapid developments expected in domestic payment systems.

Reserve Bank of India (RBI) which has taken the initiative of introducing computerisation in middle of 80's has introduced in middle 90's a special variant of EFT in the form of an Electronic Clearing System (ECS) - a clearing system meant for effecting bulk payment transactions without using paper instruments thus paving way for quick and improved customer service to banks/companies, corporations etc. ECS consists of two parts: credit clearing and debit clearing.

### 6.3.1 ECS Debit

The ECS debit system is used for transactions which involve movement of money from a large number of accounts to a single account. These transactions can be income tax payments by taxpayers, payment of bills by customers of various public utilities etc. In this system the debit information/instructions is brought to the clearing center by the sponsor bank on magnetic media for subsequent processing.

### 6.3.2 ECS Credit

ECS credit system can be used for transactions which involve multiple credits. These transactions can be payment of interest, salary, pension, dividend, refund etc. which involved movement of money from a single source to a large number of customers. Instructions/information about the credit of a customer to destination account is brought to the clearing center by the user bank on magnetic media for onward processing.

### 6.3.3 ECS Growth

During the last five years, ECS has grown both in terms of volume and number of centres. Starting with four mega-metros: Mumbai, Chennai, Calcutta, New Delhi; ECS service was extendd to four more centres: Hyderabad, Bangalore, Ahmedabad and Pune, by 1997 and by 1998 ECS has been extended to eight more centres: Bhubaneshwar, Chandigarh, Guwahati, Jaipur, Kanpur, Nagpur, Patna and Trivandrum.

The four mega centres in particular and the remaining twelve centres in general have shown phenomenal growth in the ECS traffic both in terms of volume and value. As expected the four mega centres: Mumbai, Chennai, Calcutta and New Delhi account for more than 90% of the ECS traffic.

83
6.3.4 Security and Control aspects of ECS /EFT:

6.3.4.1 Password Protection
EFT software package, supplied to the EFT-service-branches is password protected. Users are advised to change their passwords on a regular basis. There are two levels of users – “super” users and “operator” users. The operator users can change their passwords without the knowledge of super user.

6.3.4.2 Levels of User Authority
The “operator” user is allowed data entry and data correction. Unless the data file is processed by “super” user, data file of required layout cannot be generated.

6.3.4.3 Encryption
EFT Data File to be submitted to local NCC must be encrypted with the encryption key exchanged with NCC. When the EFT Data File reaches NCC, it is decrypted with the same key. This key is required to be kept confidential.

6.3.4.4 Declaration-cum-control statement
Participating banks are required to submit a declaration-cum-control statement (Form EFTR – 3A / EFTR-3B) irrespective of whether the data file is sent over the network or on floppy diskette. This is submitted by an authorised person of the participating bank. Number and value of transactions indicated on the statement is compared with the figures generated by the system from the data file transmitted/submitted.

6.3.4.5 Checksum Total
All transaction records in the, EFT Data File bear a checksum total. When the file reaches local NCC, software package at NCC checks the integrity of the data record by regenerating a checksum total and comparing with the checksum total supplied in the file. If some data elements are altered during the transmission or tampered on the floppy diskette, the checksum total would not match. In such case, EFT Data-File would not be processed and the remitting bank would be advised suitably.

6.3.4.6 Control Reports from Local NCC to the Service Branches
Service Branches of banks act as the nodal point for all outgoing and incoming transactions. Local NCC would be supplying the following three reports on a daily basis. Service branches shall scrutinise these reports and reconcile the entries on a daily basis.
6.3.4.7 Check Signal
The participating banks may mutually agree to include a check signal against every transaction and enter the check signal in the ‘remarks’ column on the data entry screen. The check signal algorithm may take into account a variety of data items to be decided between the banks. Accuracy of the check signal data-item would be checked at the remitting branch level and at the and at the destination branch.

6.3.4.8 Use of Pre-printed Continuous Stationery
All reports relating to EFT transactions generated either at Reserve Bank or at EFT service branch level shall be on pre-printed continuous stationery which will bear the name of the organisation and a serial number.

6.3.4.9 Contingency steps
In case RBInet communication links fail at a centre, movement of data-files between EFT-service-branch and NCC may take place by physical delivery of floppy diskettes. In case inter-city links for RBInet fails, NCCs would exchange RBI Data-Files through NICNET. If both, the RBInet and NICNET fail, NCCs would arrange to send through some other network or the Data-files would be sent on floppy diskette or any other magnetic media between the centres through alternate arrangements. In case an EFT-service-branch is not in a position to operate due to fire or some such disaster, another branch at the same centre can be designated as service branch for a temporary period. A backup copy of EFT software package and RBInet package should, therefore, be stored in another branch under secure conditions to meet such eventuality.

6.3.4.10 Written confirmation from service branches on contingency arrangements
NCC may obtain a written confirmation from the local EFT service branches of the contingency arrangements made by each of them.

6.3.5 Audit aspects of ECS/EFT
While auditing the EFT function at the service branch, the internal auditors / inspectors / IT-auditor should necessarily scrutinise the observance of the following security procedures:
**Password** - The EFT software provides two types of users depending on the access level. The operations carried out by the users are logged by the EFT package. Therefore, it is essential to protect the system from unauthorised entry. This, in turn, requires that the passwords used by them are carefully used. Both, the 'super' user as well as the operator user should change the password on a regular basis. The ‘operator’ can change the password without the knowledge of the 'super' user.

**User Authority** - There should be demarcation of work between the 'super' user and the 'operator' user. For any transaction to be completed, two persons should necessarily be involved.

**Encryption / Decryption** - The data file to be submitted to the local NCC is to be Encrypted giving a key and that key is to be exchanged with local NCC in confidence. It is recommended that the key should be changed at regular intervals (at least once a month).

**Verification / Reconciliation** - Irrespective of whether the data file is sent over the network or on floppy, verification of control statement should be given due emphasis. Local NCC supplies three reports:
- Report No: EFTR-1B NCC, Listing of Outgoing Transactions
- Report No: EFTR-2B NCC Listing of Incoming Transactions
- Report No: EFTR-Daily Settlement Statement

to the Service branches have to reconcile the figures on a daily basis.

**Pre-printed Stationery** - All reports relating to EFT transactions both at the Reserve Bank and the Service Branches should be on pre-printed stationery bearing the name of the Organisation and serial number.

**After transmitting the data file over the RBINet** the 'super' user should check the status of the EFT message and update the transmission status, a printout of the acknowledgement status generated by RBINet software should also be taken. This status indicates the time when NCC received the EFT message.

**Original / duplicate Reports** - Branches make payment to the beneficiary based on the hard copy credit report (Report No.:EFTR-5A) or refund the remitter of the remittance amount for the rejected acknowledgement on the basis of acknowledgement report (EFTR-5B). EFT package has been designed to generate a copy-number against every
copy printed. Branches are to act on copy number "1". Copies generated after the first copy bear the numbers 2,3,4,5 ..... onwards. If for any reason service-branches are not in a position to send the first copy and that needs to be indicated in the copy sent with duly signed certification that "copy number 1 has not been sent and that they should consider copy number--- as copy number 1" etc.

**Software packages** supplied by the Reserve Bank should be kept in a secure place preferably in the custody of the officer in-charge of the Service Branch or, the designated 'System Administrator' of the Service Branch.

**Even if there are no EFT transactions** to be reported, "Hello" messages should be sent to Local NCC on a daily basis through RBINet.

**Periodic scrutiny** may be conducted by a person other than the 'super' and 'operator' users that the data-files are not tampered and that the reconciliation is done on a daily-basis.

**Backup** - Back-up exercise as indicated below should be carried-out and recorded in a register by the 'super' user on a daily basis.

**6.3.6 Back-up Procedure for service branches of banks**

Each participating bank should have a back-up computer system so that the back-up system is made operational within an hour of the primary system going inoperative. This back-up system should be located either at the service branch itself or any other branch / office in the city. Alternatively, banks can have mutual back-up arrangements. In such cases of mutual back-up, due care should be taken on data security. Transaction files should be backed-up on a daily basis and the 'super' user for the day should record this fact in a register. Audit trail files should also be backed-up. A copy of the EFT software package and RBInet package should be in the custody of the Officer-in-Charge or System Administrator of the Service Branch. Internal Auditors / Inspectors /IT-auditors of banks should necessarily examine this aspect while inspecting / auditing the Service Branch.

**6.4 Security and Control aspects of E-mail System**

Almost all the banks in India are gradually becoming extremely dependent on e-mail. Some of the Indian banks have also been offering e-mail-based funds transfer system, for last 3-4 years. They are becoming very reliant on their e-mail systems to conduct
other day-to-day operations. If their e-mail capabilities are disrupted, it could result in
a great deal of staff inconvenience, loss of productivity, inability to provide prompt
customer service and also loss of business.

E-mail raises some unique control-issues, some of which have now become quite
evident. Many breaches of confidentiality/privacy are experienced almost daily by
various organisations, in e-mail systems.

Here are some of the control characteristics that are worthy to note:

• E-mail communication is essentially in the public domain. This means that virtually
  anyone around the world can have access to your mail if they have the means to
  accomplish it. The means to intercept e-mail are increasing all the time.

• E-mail goes through the e-mail-service-provider and may be in the domain of many
  organizations while in transit to you. It is in fact in the files/data bases of your
  service provider for potentially ready access by any insider.

• E-mail can be intercepted and compromised, unless it is thoroughly protected and
  encrypted from source to destination.

• As mentioned earlier, e-mail is subject to disruptions, as a result of breakdowns in
  your internal communication-server or external service provider, which may lead to
  serious inconvenience and a potential business outage. This can translate into a real
  loss of profits and loss of operational efficiency and effectiveness.

• The messages can be intercepted and used.

• E-mail messages can accidentally end up in the wrong destination as a result of
  address errors or similarities.

• Very important messages may often not be received by the target party which if
  critical, can end up in unawareness by the receiving party, loss of opportunity, and
  loss of business, unless some form of confirmation, or receipt were to be obtained
  by the sender.

• When indiscriminate use of e-mail is made to send sensitive information, the
  organization may place itself in jeopardy if information on such things as
  competitive bidding, business strategies, product information and planning etc.,
  falls into the wrong hands.

• There is even the potential for interception and alteration of the messages for
  whatever devious ill-design and objective that an adversary or a competitor may
  choose to play.
• E-mail messages can be misrouted or they can find their way into erroneous addresses, thus incurring the danger of assuming that the appropriate party received the e-mail message when in reality he/she may not have received the message
• E-mail messages may be lost.
• Documentation of e-mail is generally inadequate.
• E-mail can gradually cause individuals to become increasingly less-careful with maintaining proper and legal documentation and audit-trails which can cause an inability to produce a formal and structured form of documentation, evidential matter, and audit trails that can otherwise be used as official evidence in some courts or disputes
• There is no adequate legal backing for e-mail-based communication. However, after the Cyber-laws come into existence, it is expected, this issue gets sorted out in the near future. The IT-bill in this regard is already passed in the parliament, in May 2000.
• Over-use or inappropriate use of e-mail may contribute to make some types of business communication somewhat impersonal.

6.4.1 Strategies
Several strategies might be conceived and used to minimize or mitigate the potential risks of using e-mail for intra-organisation and inter-organisation communications. Perhaps, combinations of these strategies may be appropriate to achieve the desired objectives.

Using control strategies long before, one can decide to select specific control procedures that fit under the given strategies is a very useful way to visualize how the control approach would work towards the goal, of achieving the control or security objective. It will also enable to compare which of the control strategies may be most effective for the purpose at hand. For example, if the objective is to keep very sensitive company information from being intercepted over the e-mail systems, the "information classification" strategy would probably be the most effective. Therefore, the following are the suggested strategies for confidential message protection for e-mail systems.

6.4.1.1 Data/Information Classification Strategy
This may be the first and most effective line of defense. In this strategy, management should clearly mandate that certain types of "classified" information and messages are not to be sent over the e-mail system(s) under any circumstances. The premise is quite
simple. If the data is not transferred over e-mail systems, they cannot possibly be intercepted or captured - at least in that form or from that source. Naturally, this does not preclude someone accessing the message on other forms, such as on written instruments or letters.

This may include types of information such as banks' corporate plans, business strategies, various policy documents (like IT policy, IT-security policy, etc.), other documentation (e.g. system documentation, system design, etc.), source-codes of various application-software systems, confidential business-data, research-related documentation, secret-formulas/mathematical models, algorithms, key business-rules, etc.

6.4.1.2 Concealment Strategy
In this strategy, the "contents" of messages are concealed via such protection mechanisms such as checksum, encryption and data-compression.

As is true of almost all control strategies and mechanism, this does not give 100% guarantee that the messages will not be tampered with, since encryption mechanism can be broken and compromised. The "hacking" is now-a-days a profession which is growing very fast. There are cyber-underworld organizations and individuals that may possess sophisticated code-breaking capabilities. The minute that messages are transmitted by e-mail, the bank is automatically incurring the risk of interception.

6.4.1.3 Decoy Strategy - Misinformation
This strategy advocates the use of disguising, misleading messages to distract the identity of the legitimate message. Naturally, this strategy must be used with due consideration and care to ensure it does not instead awaken other potential legal or loss of trust by-product effect. The strategy may have some value when sending information by two different channels. This creates additional effort on the part of the would-be intruder in having to decide which information is in fact valid.

6.4.1.4 Containment Strategy
In this strategy, sensitive information is not only not sent over the e-mail system but it is restricted to the confines of a given business unit, department or individual to avoid careless proliferation outside the restricted circles. It is best to apply this control strategy with the "classification" strategy described earlier, as they usually go very well together.
6.4.1.5 Divide and Conquer Strategy
In this strategy, the sensitive message may be split into sections that may be transmitted by separate mechanisms or mediums, whereupon the receiving party reassembles the parts to get the full meaning of the message.

6.4.1.6 Time Division or Splitting Strategy
This strategy is similar to the divide and conquer strategy except that it is practiced across time periods in such a way that segments of information are transmitted across time lapses.

6.4.1.7 Limit Strategy
In this strategy, the "quantity" of sensitive information that is emailed is limited per session.

6.4.2 Importance of e-mail-system Audit
In view of recent developments related to careless use of e-mailing, the involvement of audit, internal-control and information security professionals is very desirable indeed. Since legal implications are arising from the improper use of e-mail, the legal officer should also become involved to assist in formulating adequate policies and practices for the sound and secure use of e-mail services.

To assist the banks in reviewing the status of e-mail-use in their offices, the following are the questions that ought to be asked in the assessment process.

- Does the bank have a formal policy that details the responsibility and accountability of branch managers/RO, RCC in-charge/ ZO, ZCC in-charge, and HO level departmental heads, and other employees to ensure that e-mail is used according to prescribed guidelines?
- Is there “information-classification” scheme that clearly outlines what types of sensitive information shall not be transmitted over e-mail systems? This classification scheme should spell out the list of bank-wide data that is not suitable for e-mailing.
- Are there instructions on how to handle the restricted or sensitive information and what channels of communication and documentation are to be used for exceptional information?
➢ Is there a set of guidelines and best practices for the sound and secure use of e-mail information; this may include even backup and recovery procedures for recovering e-mail information in case of data loss?
➢ Is there any area-supervisor responsible for disseminating appropriate practices and monitoring and updating the best practices for the sound use of e-mail?
➢ Are there audit procedures to ensure compliance?
➢ Are there regular procedures to monitor and maintain the e-mail practices to keep up with the evolution in the use of e-mail services?
➢ Are new employees briefed on the proper use of e-mail and regular employees brought up to speed up the proper use of e-mail?
➢ The policy on not sending sensitive information over the e-mail systems can be also linked to the personnel policies and the non-disclosure agreement that employees sign up with the bank/organisation upon accepting employment, and updated for employees which join the bank/organisation prior to the latest agreement. This should be made a formal part of the personnel practices on releasing or mis-handling of bank’s confidential information that may place the bank in jeopardy.
➢ Is there a bank-policy or procedure that forbids employees to use e-mail for personal purposes and or that violates any of the various regulations or laws that the bank may be obligated to observe and enforce?
➢ What are the control practices now being used for managing and harnessing the use of e-mail services? Is there a minimum of security practices? Are e-mail messages encrypted by the e-mail system in use? Are the servers that handle e-mail protected by firewalls? Are digital signatures used to authenticate servers that send or receive e-mail information?

6.4.3 Help Desk for Proper Use of E-mail

Banks often have various forms of help desks for the use of technology-oriented services. One possible consideration is to add an e-mail "help-desk" capability to one of the existing help desk capabilities to assist with issues related to advice, suggestions and troubleshooting on the use of e-mail. Such a help desk, working with human resources, legal and info-security groups, could enact a set of detailed guidelines for dissemination and for use in training sessions to help minimize the small-tasks of the average employees having to find out what the bank rules are for the use of e-mail, when it comes to regular and sensitive issues.
With the popularity of the use of e-mail for sending information around the globe and even for using it for business transactions, there are chances that e-mail facility is used in more casual ways. It is then prudent to see sensitivity, confidentiality, and potentially damaging aspects of the information, before releasing it.

All this will help bring to the attention of IT-managers, IT-auditors, IT-security professionals and legal experts to the need to develop formal policies, standards and procedures to anticipate the potential for undesirable consequences to take place as a result of indiscriminate use of the bank’s or outside e-mail services by employees including the management.

Although e-mail is a tremendous tool to expedite communications and increase productivity, it can also be a double-edged sword that may result in unwelcome consequences, especially when used to send sensitive or confidential information. Besides hackers’ inclination on obtaining unauthorized information, there lies the danger of competitors, legal and government agencies seeking evidence for prosecution or other purposes. Therefore, the involvement of computer-auditors, internal control and security professionals and the legal department is advocated to arrive at practical guidelines for a more secure use of e-mail services in their banks.

6.5 Internet-banking (e-banking):

At the moment, the Internet-banking (which is also called as e-banking) is in a very preliminary stage in the developing country like India. At present, it is just an advance version of tele-banking services which are being provided many banks in India for past 4-5 years {ref. Prof. S M Padwal, "Need for Redesigning Information Technology (IT) / Information System (IS) Architecture in banks in India", Conference of Chairmen of Banks, January 06-07, 2000, NIBM, Pune}. Many banks in India have now started using Internet basically for publishing their bank-profile and for marketing of their schemes and services. Some banks offer services like opening an account, enquiry of balances of accounts, request for cheque-books and few other similar facilities. The use of Internet for actual transaction processing is still in the experimental phase. However, as the customers demand increase in the days to come, banks may come forward to provide true e-banking services. They may even think of participating (as a financial intermediary) in e-commerce related activities.
So, for the banks in India, as the importance of Internet as a strategic resource for global reach (by its nature itself) becomes clearer on one hand and the process of globalisation accelerates on the other hand, the security related issues in such an environment should get utmost consideration. Connecting to the Internet without strong security architecture in place, can have sever consequences. The extent of criminal activities in the Internet-based environment is expected to grow with an accelerating speed. In spite of this, the precautions taken by the organisations (including banks in India) which are connected to the Internet, are amazingly inadequate. Even part-time hackers can gain access easily. However, a well-designed strong firewall architecture, can provide necessary protection against cyber-crimes.

Addressing the security aspects of Internet-based banking requires analysis of at least the following issues:
- potential risks of being on the Internet,
- security-weaknesses in such an environment, and
- Cyber-Crimes and Hacking.

6.5.1 Being on the Internet
The potential risks to the banks from being on the Internet (over and above the risks discussed so far) involve:

- Unauthorised access to the information system from the outside (if technically feasible)
  - Loss of data (insertion / deletion / modification / corruption etc.)
  - Loss of confidential information (disclosure, competition)
  - Problems inherent in an open (and insecure) Internet (Viruses, Sabotage, Hacking)
- “Trojan Horses” and viruses sneaking in through transferring data on the Net (i.e. Internet)
- Using false identities (address spoofing, using third-party Ids, etc.)

In addition to this, Internet itself and ISP (Internet Service Provider), like other IT-Service Provider discussed earlier, poses risks to the bank.
6.5.2 Security Weaknesses and Attack Points

Because the Internet as a whole is so complex, as are the hardware and software components that make it up, the system as a whole is riddled with programming and operating defects. Clearly, there is no way without going to inordinate lengths of testing programs of ten thousand lines and over to ensure that they will work perfectly under all conditions. This means that any commercial software runs the potential security risk of someone taking advantage of programming errors. When the components concerned are accessible to large number of users via a computer network, the risk of isolated weaknesses being misused multiplies.

6.5.2.1 Faulty Software-design

One of the main reasons why there are so many security problems on the Internet is the basic architecture of the TCP/IP and UDP protocols. Neither of them was developed originally with the intention of ensuring really secure communications paths. When sending data via the Internet using TCP/IP, for example, there is no way of knowing by which nodes the transmission will be routed. If hackers succeed in installing so-called "sniffer" programs at one or more nodes, any passwords sent in plain text will be disclosed.

Another reason why hackers are so successful is that system configurations are poor, and that there are few or no safeguards on Internet access systems. In purely technical terms, there are five areas of weakness: lack of safeguards (no firewalls), poorly configured and administered systems, basic security problems with communications protocols (IP, TCP, UDP), faulty service programs, and basic security problems with service programs (e.g. WWW, FTP etc.), and reliability and integrity of applications based on them.

6.5.2.2 Internet-based bank as security risk

Apart from purely technical problems, many of the reasons why security standards are so poor are to be found in the organization of Internet-based banks themselves. No security officers, no focus on further training for systems managers and little or nothing in the way of internal security guidelines. This means a lot of care should be put into formulating a security strategy and in implementing the security measures. This strategy can then be used as the basis for appropriate organizational action and ultimately the procedures for implementation.
According to the hit list of the CERT- (Computer Emergency Response Team)-
coordinating-center at the Carnegie Mellon University in Pittsburgh, so-called "sniffer
attacks" are number one on the hit list of most successful break-in methods. These use
"invisible" miniature programs smuggled in on Internet hosts to monitor data flows and
retrieve passwords and system IDs.

Another trick that is used almost as often is IP-spoofing. The attacker gives his own
data packets addresses which are in the address range of the target net- work and that
therefore appear to have been generated by users on that net- work, hence the term
"spoofing." This is mainly used to overcome packet filters and proxy firewalls whose
authentication measures are based on Internet addresses.

In third place on the hit list, are attacks that use faults in the mail server application
"sendmail," which exploits three different weaknesses in the program. In fourth and
fifth place are attacks via NFS (Network File Systems) and NIS (Network Information
Service) applications.

The various threat scenarios can be broken down into five areas:

Access control management (authentication systems)
Communications protocols (IP, TCP, UDP)
Internet applications (Telnet, DNS, etc.)
Information services (WWW, Gopher, FTP) and
Computer viruses.

6.5.3 Cyber-Crimes and Hacking
As the Internet becomes a strategic resource for conducting banking activities, it opens
up the market to professional cyber-criminals and hackers. In fact, Cyber-Crime and
Hacking are professions by themselves, which are growing very rapidly. Some of these
are recruits from the computer-underworld and some are paid Internet-specialists.
These professional hackers are given concrete tasks of doing undesired/unethical/destructive things as quickly as possible. These hackers and cyber-
criminals often consult underworld Bulletin Boards to find out how to get into the
system they want. As mentioned earlier, the dramatic increase in the economic
importance of the Internet makes it to appear that the number of cyber-criminals and the
eyer-crimes / hacking they commit is increasing at the same rate. One reason, the
number of (undisclosed) successful break-ins into corporate networks is so high that
so far most of the hackers have come from relatively less-harmful computer underworld. Once they broke into a system, they left as silently as they had come in, without doing any significant damage in many cases so far. However, the hacking world is changing very fast. Increasingly, it is being populated by cyber-criminals whose only aim is to sell their sophisticated technical skills to the highest bidder (criminal). In most of the Indian organisations (including banks) those which are on the Net, the corporate IT-security arrangements are often so preliminary that even weekend hackers find it easy getting into a system.

In order to emphasise the importance and seriousness of computer-crime and hacking-related issues in such environment, we are giving below a few of the major computer-crimes and hacking events occurred in this decade in the advanced countries.

During 1993, IEEE (Institute of Electrical and Electronic Engineers, USA) discovered sniffer-programs on an Internet-gateway-computer-system, which monitored and saved login-ids and passwords automatically. Initial estimates reckoned that over 1,00,000 passwords were captured.

At&T (USA) reported that Telephone fraud costed them over 2 Billion US$ during 1993.

In 1994, Martin Janku, an employee of Czech savings bank in Sokolov, was sentenced for eight years’ imprisonment in the first major case of computer-crime in the Czech Republic. He had transferred 1.2 M US$ to his account using a computer-program which he himself had written.

In February 1995, the FBI (Federal Bureau of Intelligence, USA) caught Kevin Mitnick (31), “Wanted No.1 Hacker”, after a two-year man-hunt. He was accused of stealing thousands of files and unlawfully using over 20,000 credit-card numbers.

In July 1995, Vladimir Levin, a Russian, managed to siphon-off 90 million US$ from Citibank of New York and other banks (collectively).

There may be many other computer-crimes and hacking events which are not detected so far, or detected but were not made public for various reasons. Therefore, the real extent of seriousness of this issue is something we can only speculate about.
In view of this increasing danger, the Committee on Technology Upgradation in the Banking Sector, which was setup by RBI under the chairmanship of Dr. Vasudevan (ED, RBI), has suggested that the Tiger Teams (Hackers Team) should be developed to determine strength (and especially weaknesses) of the Firewalls and other Internet-based systems. {ref. Report of the Committee on Technology Upgradation, July 1999, para. 3.2.8}.

6.5.4 Internet Security Design and its Implementation

The first step when setting up a network security system is to establish Network Security Policy and lay down appropriate corporate guidelines (refer Appendix 3 for Sample Network Security Policy). These then serve as the basis for an implementation plan that can be translated into reality.

6.5.4.1 Corporate guidelines for network security

The corporate guidelines state what the bank requires in terms of the proper use of computer systems and data networks. They define ways of preventing violations of those rules and what to do if a breach occurs. The main thing about security guidelines is that they must not go against current law or other existing corporate guidelines/works agreements.

a) Goals

The starting point for producing corporate network security guidelines is usually to make an overall definition of how data networks and computer systems work and what they do. This specifies what services are to be provided and what security and availability requirements the information technology has to meet.

To the banks and other financial institutions, network security required is something considerably different from that in most small companies. This means that the overall network and security objectives depend mainly on the nature of the organization concerned. What is important is that the guidelines produced should be technically and commercially feasible, and should be backed up by the management. The contents should be devised in talks between IT-staff on the one hand and management on the other. It is also necessary to indicate who is responsible for interpreting guidelines in each case.
b) Risk analysis

To ensure that the measures defined in the corporate guidelines are realistic, the first step is to draw up as detailed risk analysis as possible. The assessment of

- what is to be protected
- who it is to be protected against, and
- how (well) it is protected

provide the basis for an appropriate security strategy. Both inadequate security precautions and exaggerated ones can have serious financial implications for banks.

Identifying objects to protect is one of the main tasks in this early stage of security planning. Any errors here will affect the entire strategy and usually leave major security gaps. The list given below may help in covering them:

1) **Hardware**: Workstations, PCs, keyboards, printers, disk drives, networks (LANs, WANs, Internet), terminals, routers, bridges, etc.
2) **Software**: Source code, executable programs, diagnostics software, operating systems, communications software, games, etc.
3) **Data**: Data while executing software, data saved online, data filed offline, backup data, data from monitoring software, data while sending via e-mail/Internet, private data, etc.
4) **People**: Users, system managers, guests, consultants, service staff, etc.
5) **Documentation**: Program documentation, hardware documentation, system management documentation etc.
6) **Accessories**: Printers, disks, tapes, etc.

Once we have defined the objects to be protected, we can start setting up potential attack scenarios and assessing their impact on the bank. These fall into three main categories:

- Penetration by unauthorized persons
- Disrupting the network
- Loss of confidential information.

c) Formulating security guidelines

By using the results from the risk analysis, we can now start formulating the security guidelines (similar to approach that we used during this study). Security guidelines for
people should define the rights and obligations of everyone user of the network. In most banks, these will include:

- Staff
- Visitors and temporary staff
- Systems managers
- Service staff and outside consultants
- Customers (who are receiving Net-based services)

As a rule, guidelines that cover all staff are gathered under the heading "General rules for using network-based systems". The questions are:

Who is authorized to use what systems or services?

What do we mean by authorized use of systems or services?
- Not getting into outside systems
- Not capturing passwords
- Not reading or tampering of other people's files
- Not sharing your account with other people or staff No copying copyright software

Who is authorized to set up system access (user accounts) for users?

What are the duties of system users?
- Keep users passwords secret
- Change passwords regularly
- Make backup copies of your own files
- Keep secret data secret
- Follow the guidelines for using system resources (memory space, etc.)
- Follow guidelines for using the internet
- Adhere to guidelines for using DP systems for private purposes
- Monitor your own account for unauthorized use.

The people who have the most (in practice, usually unlimited) rights in terms of the IT-infrastructure are systems managers. What people often forget is, this means they are also potentially the greatest threat to the system. So as well as choosing people carefully, it is essential to define systems managers' jobs, their rights and duties. Typical problem areas that should be tackled are:

- Who is authorized to receive systems manager rights (super-user access)?
- Who allocates those rights?
• On what basis are user rights granted (basic rule is never give users more rights than they need to do their job).

• To what extent is the systems manager authorized to analyze user data in diagnosing problems?

• Does the system administrator have the right to monitor individual systems or the network as a whole?

The best way of ensuring that security guidelines are followed is to train the people concerned and make regular checks to see that the guidelines are being followed. A comprehensive security strategy should also include further training for staff on Data and Network Security and Security Audits.

The best security measures in the world are not so useful if the hardware components that make them up are not protected properly. Guidelines for protecting IT systems should be divided into two categories:

• safeguards for individual hardware components (servers, routers, terminals, system cabinets, etc.) and

• safeguards for the company as a whole (fire alarms, water alarms, air-conditioning systems, etc.)

All the critical components of IT infrastructure (such as File servers, Application servers, root terminals, routers, bridges, remote terminals, etc.) should be protected against theft, power-interruption, excess voltage, excess temperature, unauthorised intruders etc.

One area that is very important in terms of security but that is often over-looked is control cabinets. Very often, they are installed unprotected at central locations in a building without any serious access controls being used. This means anyone can easily get at hubs, bridges, routers or cable terminals.

Checking the application-software systems the bank uses is another major component of a total security strategy. Computer systems configured individually by local-users are often the targets for external or internal hackers, or lead to data being lost, inadequate backups and compatibility problems. Privately installed applications or computer-games can open the way to viruses and Trojan horses. So the system-management must
be aware of and properly document how each computer system is configured and what the components of the network are. Time to time changes required in the system-configuration should be done only by authorized people. Lastly, the protection of user data should be given top-most importance by having a systematic backup strategy.

Before the user is allowed to access a service, you need to define whether (and if so to what extent) confidential data are likely to be involved. There is no point in saving such data on systems unless those systems are suitably protected. So users must be told what data is to be regarded as confidential and how to deal with it. The questions to ask here are:

- What data is to be regarded as secret or confidential?
- What levels of classification are there?
- Which users have access to that data?
- What services involve or enable access to confidential data?
- What systems can that data be saved on?
- What security checks apply to those systems?
- How is confidential data sent over data lines (encryption)?
- How are backup copies of confidential data kept?
- How are printouts of confidential data kept/disposed of?

Setting up outside data links, while at the same time keeping the network secure, is one of the hardest tasks, especially if the banks are linking up to the Internet. There are three basic guidelines the banks should follow when setting up outside data links:

- The banks must guarantee the security and integrity of their own in-house network.
- The banks must keep the risk of unauthorized people getting in via outside data links to a minimum.
- At the same time, the security measures used should not restrict staff from using outside services.

The security guidelines should also include a detailed list of the services available and the user groups authorized to use them. These can then be used as the basis for setting up the firewall system. The security guidelines for using the Internet include:

- Any Internet services not expressly authorized must be disabled
- Registered and authorized users should have access to the following Internet services like: WWW, FTP, e-mail, Gopher, Archie.
• Non-registered and unauthorized users cannot access the Internet. Access management is via a dedicated firewall system.
• There must be no direct links between the bank's in-house network and the Internet. The only access to the Internet is via the its firewall system.
• The firewall system must have monitoring and alarm systems for detecting breaches or impending breaches of security rules (outside attacks, changes in configurations, breaches of data integrity, etc.).

If the system administrator or IT-security officer or IT-auditor finds that there has been a breach of the security rules, it helps to have countermeasures already in place. This means the corporate guidelines should have a separate section telling people what to do in the event of different security incidents. Basically, there are two very different strategies that can be used: 1) Protect and continue working and 2) Catching and punishing.

In many cases, it may be best to use a combination of the two, depending on how serious the breach is. The aim of the "protect and continue" guideline is to ensure that things get back to normal as soon as possible once the breaches of security have been plugged. The "catch and punish" strategy involves allowing the security rules to be breached (preferably in a controlled fashion) until the offender is caught. In addition to the experienced systems and network specialists who look for the offender, however, this also involves being ready to accept further breaches of security and hence ultimately of losing data. The following guidelines may help in choosing the appropriate strategy:

i) Using the make safe and continue strategy:
• Data and computer systems are inadequately protected
• Further breaches of security are an incalculable risk
• You are not prepared to put resources into bringing charges against the offender
• You don not know exactly who is in what user group
• Users are unfamiliar with computing

ii) Using the catch and punish strategy:
• Data and computer systems are adequately protected.
• You have backup copies available for all the areas concerned.
• The risk of damage from further breaches of security, which you are prepared to accept to catch the offender is reasonably proportional to damage from possible future offenses.
• The attacks are frequent and massive; the bank's internet-communication-server itself is an attractive target for hackers and is frequently subject to security breaches.
• You have experienced network managers and sufficient monitoring tools available.
• The management is prepared to pursue and punish offenders.

Evidence shows that many breaches of security rules occur unwittingly or through the negligence of the internal staff. Bringing criminal charges is usually inappropriate in these cases. Alternatively, therefore, the banks should think about specific training for this type of security incident or consider disciplinary action in serious cases.

6.5.4.2 Implementing an Internet Security Architecture

Now that we have looked at corporate network security guidelines, it is possible to create the security architecture itself. To do this, it is necessary to convert the corporate guidelines into a detailed working draft. In the next stage, the implementation phase, this functional architecture will be installed, tested, and put into use. Some security guidelines may involve organizational changes and structural measures as well as technical changes.

a) Designing a functional Internet security architecture

Designing a working security architecture is based on the dictates of the existing IT-infrastructure such as: Operating system, Network topology, Network protocols/Network-operating systems, and Outside data links/communications protocols.

On this basis, the next step is to find a solution for each of the services required. From these solutions as a whole, one can ultimately build up a firewall-architecture and detailed specifications for the security system. From this specification, it is possible to choose the products (refer Appendix 4 for list of Firewall products) for creating our proposed security system and, after a risk analysis of the firewall configuration (cost/risk assessment), thus one can decide on how the final security system will look.
Therefore, planning and implementing a firewall system include the following milestone:

- Corporate guidelines
  - Risk Analysis
  - Formulation
- Implementation
  - Working security architecture
  - Solutions
  - Cost/risk assessment
  - Selecting systems
- Implementation

b) Implementing the firewall system

At first, the firewall components are installed completely separate from the operating network and subjected to a series of tests. The results of the working and integration tests are fed back into the design of the system as a whole until it is working satisfactorily. The implementation phase finishes by producing the full documentation and putting it on the network.

c) Introducing working procedures

Introducing reliable operating procedures for the security system is just as important as implementing the firewall system itself. This should be based on the documentation of the security-architecture, consisting of the three components: System documentation, Operating documentation, and Logbook.

System documentation should include information of importance to all systems managers such as: Network configuration, Firewall configuration, Internet services configuration, and Documentation of installed monitoring and alarm systems.

Operating documentation should contain descriptions of all operations that have to be used while using the different firewall components. These include: Making backups, Maintenance (DNS, etc.), Analyzing and interpreting the different monitoring and alarm systems, Instructions for shutting down/starting up the system, What to do if operating problems occur, and What to do if there is a security breach. Lastly, the logbook should record everything the systems manager and other users do.
6.6 Some of the emerging Electronic-Money Products and Services
As mentioned earlier, the world of e-banking (i.e. Internet-banking) is still in its infancy. There are many electronic-money transfer products coming on the market. There is no way to predict which system will emerge as the favorite. In India, only a few banks have made just made a little beginning on a pilot-basis towards providing preliminary services related to e-banking. However, as the customers demand increase in the days to come, banks may come forward to provide true e-banking services. Therefore, the researcher had done the comparative study of various electronic-money products and services available today in the market. Table 6.2 (on the next page) shows the comparison of some these products covering various aspects like whether it is Online or Off-line, Security features, use of digital certificates, and anonymity.

6.7 Conclusion
In this chapter, it was attempted to discuss the security and related aspects of some of the banking-technologies emerging in the Indian banking industry. Though we are moving ahead in the deployment of state-of-the-art technology in banks in India, there are many issues related to IT-security and IT-audit of the existing IT in the banks. In the next chapter, it is attempted to discuss these issues and suggest some remedial actions.
Table 6.2: Comparison of some of the emerging Electronic Money Products

<table>
<thead>
<tr>
<th>Sr. #</th>
<th>Product</th>
<th>On/Off-line</th>
<th>Security/ Encryption</th>
<th>Certificates</th>
<th>Anonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>First Virtual (uses no cryptography, certificates or digital signatures)</td>
<td>On-line for verification of A/C number. Off-line for back-office transactions</td>
<td>e-mail Security. Stops the repudiation through social-force of closing down the A/C of people who deny too many transactions.</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>2</td>
<td>iKP (i.e. 1KP, 2KP, 3KP) (requires central clearing-server for authorisation)</td>
<td>Must have complete On-line connectivity with the central-server</td>
<td>Yes, at the transaction site. Public-key encryption.</td>
<td>1KP uses certificates for the bank only. 2KP uses certificates for merchant also. 3KP requires certificates for bank, merchant and customer also.</td>
<td>The bank knows the identity of both, the merchant and the customer.</td>
</tr>
<tr>
<td>3</td>
<td>NetCash (Requires central-server to authenticate coins)</td>
<td>On-line</td>
<td>Yes</td>
<td>Currency-server uses Public-key certificates. User doesn't need certificates.</td>
<td>Optional</td>
</tr>
<tr>
<td>4</td>
<td>NetCheque (Requires central Kerberos Server to generate Kerberos tickets)</td>
<td>On-line central-server to generate transaction key.</td>
<td>Yes</td>
<td>Through Kerberos system. Doesn't use public-keys for certificates.</td>
<td>NO</td>
</tr>
<tr>
<td>5</td>
<td>CyberCash (This product is just a front-end for credit-card and bank transactions.)</td>
<td>On-line. Bank- server confirms or denies the transaction.</td>
<td>Yes, uses full 768-bit RSA as well as DES encryption. All transactions are authenticated with MD5 and 768-bit RSA signatures.</td>
<td>Public-key based mechanism similar to certificates, is used.</td>
<td>Limited Anonymity. Less than that in Credit-card based systems.</td>
</tr>
<tr>
<td>6</td>
<td>CheckFree (Transactions can be prescheduled. Total transaction-cycle time is about 4 days.)</td>
<td>Works in Off-line mode.</td>
<td>Security Yes. However, NO encryption is used here.</td>
<td>NO</td>
<td>NO. This product is used for the payment of periodic (e.g. monthly) bills.</td>
</tr>
<tr>
<td>Sr. #</td>
<td>Product</td>
<td>On/Off-line</td>
<td>Security/Encryption</td>
<td>Certificates</td>
<td>Anonymity</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>7</td>
<td>OpenMarket (Designed for building a store)</td>
<td>On-line</td>
<td>Yes, Flexible mechanism for encryption.</td>
<td>-----</td>
<td>NO</td>
</tr>
<tr>
<td>8</td>
<td>CAFE (Smart-card based system)</td>
<td>Off-line with central-server</td>
<td>Yes</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>DigiCash (No central certificate structure is used)</td>
<td>Requires On-line connectivity with DigiCash Wallet</td>
<td>RSA</td>
<td>Digital Signatures</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>SET (This product is a front-end for credit-card system)</td>
<td>Can be either On-line or off-line with the central-server</td>
<td>Public-key encryption.</td>
<td>Yes</td>
<td>Optional</td>
</tr>
<tr>
<td>11</td>
<td>Millicent</td>
<td>Basically On-line, but can work in off-line with the central-server</td>
<td>Through Hash-functions. Each use has a “secret” value.</td>
<td>Does not require public-key certificates.</td>
<td>NO</td>
</tr>
<tr>
<td>12</td>
<td>Citibank-Smartcards</td>
<td>Off-line with the central-server</td>
<td>RSA</td>
<td>Yes, smart-card contains certificate for the person.</td>
<td>NO</td>
</tr>
<tr>
<td>13</td>
<td>PayWord</td>
<td>Both</td>
<td>Through Hash-functions. Each use has a “secret” value.</td>
<td>NO</td>
<td>Optional</td>
</tr>
<tr>
<td>14</td>
<td>MicroMint</td>
<td>Both</td>
<td>Through Hash-functions. Each use has a “secret” value.</td>
<td>NO</td>
<td>Optional</td>
</tr>
</tbody>
</table>

* * *