6. SECURITY ISSUE AND DISASTER PREPAREDNESS

We need to secure banking system of India. To secure banking system means to protect it from all the odds like banking frauds, cyber crimes, information leakage within the bank and many more. There is no end of these odds, the list goes on and on as day by day new type of security issues can be heard of. PSBs are at par with Private Sector Banks in terms of providing security to Customer Information, Internal Process and Infrastructure of the bank. They are using latest technologies to provide one of the best banking services to their customers around the globe. Banks are spending huge amount of their budget on data security by having data centers and different cosmic zones, Replication of data on servers, fast and efficient Data Warehousing and Data Mining Tools, Updated Databases of latest versions, more ATM outlets in rural areas, Fast and Customer Friendly Internet and Mobile Banking. Let us have a look on security which banks provide to its Customers, Internal Process and Infrastructure.

6.1 Security Issues in Public Sector Banks

Information Security

According to Peter F. Drucker-“The diffusion of technology and the commoditization of information transform the role of information into a resource in importance to the traditionally important resources of land, labor and capital.”

Information and the knowledge based on it have increasingly become recognized as ‘information assets’, which are vital enablers of business operations. Hence, they require organizations to provide adequate levels of protection. For banks, as purveyors of money in physical form or in bits and bytes, reliable information is even more critical and hence information security is a vital area of concern.
Robust information is at the heart of risk management processes in a bank. Inadequate data quality is likely to induce errors in decision making. Data quality requires building processes, procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. *The fundamental attributes supporting data quality should include accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, and usability and audit ability.* The data quality provided by various applications depends on the quality and integrity of the data upon which that information is built. Entities that treat information as a critical organizational asset are in a better position to manage it proactively.

6.2 Security Attacks

Phishing

Phishing is one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links to enter their information, and so they remain unaware that fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. In some cases, pop-up windows appear in front of a copy of a genuine bank website. The real web site address is displayed; however, any information that is typed into the pop-up directly goes to unauthorized users. In recent times, phishing incidents have been attempted using the names of Reserve Bank of India/IBA to target gullible people. *On 27th Aug 2012 Zee News showed news on phishing. Attackers sitting thousand km away from India are accessing Indian customers accounts easily. This was done using an information reader in ATM machine*
Cross-site scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injections by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward. The term is a combination of 'voice' and phishing. In Vishing, a scammer calls and pretends to be a bank representative seeking to verify account information, thus exploiting the public's trust in landline telephone services. It is typically used to steal credit card numbers or other information used in identity theft schemes from individuals. Example: BOB manager got a call from a fraudster to transfer amount in his personal account immediately. The fraudster pretended to be DGM of the bank. After transferring the amount it was withdrawn within half an hour in different locations of the India.

Cyber Squatting

Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. Cyber Squatters register domain names identical to popular service providers’ domains so as to attract their users and benefit from it. This is an issue that has not been tackled in the IT Act, 2000.

BOT (Build, operate and transfer) Networks

A cyber crime called 'Bot Networks', wherein spymasters and other perpetrators of cyber crimes remotely take control of computers without users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as
‘Trojan horse’ sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them gets activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks.

‘Trojan horse’ provides a backdoor to the computers acquired. A 'backdoor' is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Bot Networks create unique problems for organizations because they can be upgraded remotely with new exploits very quickly, and this could help attackers pre-empt security efforts.

**Denial-of-service attacks**

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently. A denial-of-service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service (DDoS) attack, large numbers of compromised systems (sometimes called a Bot net) attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying the service of the system to legitimate users.

Although a DoS attack does not usually result in theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular
network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial-of-service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced websites accessed by millions of people to temporarily cease operation. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks and credit card payment gateways. The telephony denial-of-service (TDoS) attack is a new kind using telecommunications, particularly attempted in the western countries.

The TDoS attack is a way to divert a victim’s attention from what is really going on, and a way to make the victim unavailable to banks and other financial institutions. In this scheme, fraudsters try to change the victim’s profile information by contacting financial institutions (i.e. email addresses, telephone numbers and bank account numbers). Fraudsters then use automated dialling programs and multiple accounts to overwhelm victims' cell phones and land lines with thousands of calls. When victims answer the calls they hear nothing on the other end, an innocuous recorded message, advertisement, or a telephone menu. Calls are typically short in duration but so numerous that victims in some cases change their phone numbers to terminate the attack. These TDoS attacks are used as a diversion to prevent financial and brokerage institutions from verifying victim account changes and transactions. Fraudsters thus get adequate time to transfer funds from financial online accounts.

**Pharming**

Pharming or Pharming is typically a DNS (Domain Name System) attack commonly called DNS Poisoning. If the system is infected with a 'Virus' that poisons the DNS system, whenever the victim next visits online banking site, he/she may not be directed to the actual web page, instead sent to a false 'Pharming Page'. 
Insider threats

Given the extensive use of Information Technology by banks, the risk of unauthorized access, disclosure and modification of information by insiders or employees of banks is high. Even unintentional errors could have undesirable implications. There is a need to institute robust security processes to mitigate such threats.

Malware

Malware is the term for maliciously crafted software code. Special computer programmes now exist that enable intruders to fool an individual into believing that traditional security is protecting him during online banking transactions. Attacks involving malware are a factor in online financial crime. It is possible for this type of malicious software to perform the following operations:

Account information theft

Malware can capture the keystrokes for your login information. Malware can also potentially monitor and capture other data you use to authenticate identity (like special images or words).

Fake website substitution

Malware can generate web pages that appear to be legitimate but are not. They replace a bank’s legitimate website with a page that can look identical, except that the web address will vary in some way. Such a “man-in-the-middle attack” site enables an attacker to intercept user information. The attacker adds additional fields to the copy of the web page opened in the browser. When an individual submits the information, it is sent to both the bank and the malicious attacker without his/ her knowledge.
Account hijacking

Malware can also hijack the browser and transfer funds without one’s knowledge. When an individual attempts to login at a bank website, the software launches a hidden browser window on the computer, logs in to his/her bank account, reads account balance, and creates a secret fund transfer to the intruder-owned account.

6.3 Email-related crimes

Email spoofing

Email spoofing refers to email that appears to have originated from one source when it was actually sent from another source.

Email Spamming

Email 'spamming' refers to sending email to thousands and thousands of users - similar to a chain letter.

Email bombing

E-mail 'bombing' is characterized by abusers repeatedly sending an identical email message to a particular address.

Sending malicious codes through email

E-mails are also used to send viruses, Trojans etc. as attachments or by sending the link to a website which downloads malicious code when visited.

6.4 Disaster Preparedness in Public Sector Banks

Technology is a branch of knowledge that deals with the creation and use of technical means and their interrelation with life, society and environment. The power of technology is used for material gains. It is used in mobiles, computers, TV, microwaves, at home for fast results. It is also used in banks in computers, servers, web sites to deal with day to day banking transactions. Technology means, the way of performing activities with more
efficiency in lesser time with improved skills. It may be machine, it may the process.

In a Bank hundreds of activities take place daily and these include thousands of transactions. Transactions can be relate to Check, Payment, Deposit, Transfer In, Transfer Out, Credit Card(Pay Bills), Investment, Loan, Saving account, Current account etc. to manage these transactions banks require applications to satisfy their customers fully. And these applications run on some technologies.

Technologies (struts, SAP, mainframes etc… are based on computer languages like java, .net, Cobol etc… These languages have set commands which are given to computer to function in a specific manner. Collection of commands is called a program and collection of programs with interface, input and output is called an application.

The word disaster means some mishap or damage occurring suddenly, causing loss to humans, buildings, organizations, data, connectivity, information, machines. Disaster means interruption in normal working of a system, human, machine.

When disasters take place technologies are first to be affected. On the contrary, disasters can be controlled by the technology itself. Disasters can be natural and human. Natural disasters like flood, earth quake, cyclones, volcano, drought etc… and Human disaster like Banking Frauds, Terrorism, Hardware Failure, Software Failure, Network Failure, Electricity Failure.

Suppose there is flood in the city and because of that there is no electricity. No electricity means, no computer and no computer means, no application. The customer who has urgent work in bank has to wait for hours till electricity comes or some alternative arrangements are made available to
complete their banking transactions in a smooth way. Thus Natural disasters can cause Technological disasters.

Due to Terrorism the World Trade Centre attacks Sep11 2001 more than 50 domestic and international organizations were affected. These organizations include brokerage house, a bong house, international or domestic commercial banks. They were physically collapsed completely but because of contingency planning they could be placed into operation immediately upon the destruction. Thus we can conclude that terrorism also causes technological disasters. Banking frauds like cyber crimes, forced thefts etc are also increasing these days causing harm to ATMs, banks, and society.

6.5 Increasing Concerns on Security
1. Browser Weaknesses -
   Trojans and other malware, hijack the transaction inside the browser session, attack application and database on the server. Most of the top 100 banks of the world are reported to have experienced similar incidents.

2. Consumers as endpoints -
   Banks deliver services to business customers through the browser. They are not in control of the customers computing environment. Many banks provide services to small business on consumer systems with inadequate security for business activity.

3. Multi-Channel Banking
   A cyber threat environment is growing more complex these days. Web banking expands from web and file transfer to mobile/smart phone. An integrated multi-channel approach to information, transactions and fraud is necessary to lower costs and increase effectiveness.
4. **Single Sign On (SSO)**

Banks are seeking novel corporate/business portal solutions or independent SSO applications to solve the security usability problem.

4. **Organized Crime**

Internet fraudsters have created an end-to-end supply chain to advance malware attacks and the online vector used to efficiently deploy. While the security technology market is creating security-as-a-service solutions, criminals are creating fraud-as-service activities and fraud has moved from the consumer to businesses that initiate payments and bank online. This is a huge potential for damage to national security through cyber attacks. Internet is a means for money laundering and funding terrorist attacks in an organized manner.

Management means handling something in a systematic and efficient way with the full control over activities in a right direction & restoration of normal situation in minimum time with minimum loss to the users. Objects of an effective disaster management are security in operation, safety from attacks, continuity in working & providing alternative arrangements within minimum time.

6.6 **Basic Principles of Information Security Infrastructure Related Security**

**Network Security**

1. Protection against growing cyber threats requires multiple layers of defences, known as *defence in dept*. As every bank is different, this should be based on a balance between protection, capability, cost, performance and operational considerations. Defence in depth for most banks should at least consider the following two areas.
   a. Protecting the enclave boundaries or perimeter
   b. Protecting the computing environment
2. Enclave Boundary is the point at which the organizations network interacts with the internet. To control the flow of traffic through network borders and to police its content looking for attacks and evidence of compromised machines, boundary defences should be
   - Multi-layered
   - Relying on fire walls
   - Proxies
   - DMZ perimeter networks
   - Network-based Intrusion Prevention systems
   - Intrusion Detection Systems

3. Boundary lines between internal and external networks are diminishing through increased interconnectivity within and between banks and use of wireless systems. These blurring lines sometimes allow attackers to gain access inside networks while by passing boundary systems. Still effective security deployment still relies on carefully configured boundary defences that separate networks with different threat levels, different levels of control.

   Effective multi-layered defences of perimeter networks help to lower the number of successful attacks, allowing security personnel to bypass boundary restrictions.

4. For securing large network, it is divided into large security domains. Banks must map and configure the network to identify and control all access points before establishing security domains. Network configuration considerations can include the following actions:
   - Identify applications and systems accessed through network
   - Identify all access points to network including telecommunication channels like Ethernet, Wireless, Frame Relay, Dedicated Lines, Remote Dial Access, Extranets, and Internet.
Security Issues and Disaster Preparedness

- Map internal and external connectivity between various network segments.
- Define minimum access requirements for network service.
- Determine the most appropriate network configuration to ensure adequate security and performance of bank.

Banks can avoid security threats by

a. Minimizing access to less trusted domains
b. Employing encryption
c. Controls for less secure connections

Determine the most effective deployments of protocols, filtering routers, firewalls, gateways, proxy servers and physical isolation to restrict access.

6.7 De-Militarized Zone

By placing each zone in their own security domain called De-Militarized Zone banks can restrict access to vulnerabilities. Security domains are bounded by perimeters. Typical perimeter controls include

- Firewalls operating at different network layers
- Malicious code prevention
- Outbound filtering
- Intrusion detection and prevention devices
- Controls over infrastructure services such as DNS

Consolidation on a single device could improve security by reducing administrative overhead. But consolidation increases risk as some functions cannot be performed because of reduced ability and single point of failure.
6.8  Network Protection Devices

a.  Firewalls

- Main Purpose → Access Control
- By limiting inbound (from the internet to the internal network) and outbound communications from the internal network to the internet) various attack vectors can be reduced.
- They provide additional services like Network address Translation and Virtual Private Network Gateway. Banks have four firewall types
  a.  Packet Filtering
  b.  Stateful Inspection
  c.  Proxy Servers
  d.  Application Level Firewalls

- Selection of firewall type is dependent on may characteristics like
  a.  Amount of traffic
  b.  Sensitivity of systems, data applications

**Firewall Policy**

The firewall policy should include

- Firewall topology and architecture
- Type of firewall being used’
- Physical placement of firewall components
- Permissible traffic and monitoring firewall traffic
- Firewall Updating
- Coordination with security monitoring and intrusion response mechanism
- Responsibility for monitoring and enforcing firewall policy.
- Protocols and applications permitted
- Regular auditing of a firewalls configuration
Testing of the firewalls effectiveness and good firewall related practices include:

a. Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed.

b. Using NAT and split DNS to hide internal names and addresses from external networks

c. Using proxy connections for outbound HTTP connections and filtering malicious code.

d. Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing and maintaining all software on the firewall unit.

e. Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP(Internet Control Messaging Protocol)traffic.

f. Backing up firewalls to internal media and not to servers on protected networks.

g. Logging activity, with daily administrator review and limiting administrative access to few individual

h. Using security monitoring devices and practices to monitor communications allowed through the firewall.

i. Administrating the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices and monitoring all administrative access.

j. Making changes only through well administered change control procedures

6.9 **Intrusion Detection System (IDS)**

Goal of IDS is to identify network traffic in near real time IDSs use signatures to detect port scans, malware and other abnormal network communications.
Ideal place for IDS is external to the bank as well as internally, just behind the firewall.

In this way bank can monitor the traffic appropriately towards it and the traffic that successfully passed through the firewall.

Internal traffic which tries to communicate externally to the network is also monitored. This happens when malicious activity originates from inside the firewall.

To use IDS on network IDS (NIDS) effectively, banks should have sound understanding of detection capability, effect of placement, tuning and other network defences on detection capability.

6.10 Signature based detection methodology

It reads network packets. Compares content of the packet against signatures or unique characteristics of attacks. When a match is found between current readings and a signature, IDS generates an alert. Weakness of this methodology is

Signature must exist for alert generation
Signatures are written to
a. capture known exploits
b. alert to suspected vulnerabilities

“Tuning” means creation of signatures and alert files. They can differentiate between network and malicious traffic. Proper tuning is essential for reliable detection of attacks and priority based response. If IDS is not properly tuned, the volume of alerts it generates may degrade the intrusion identification and response capability.

Behavior based anomaly detection: This method creates a statistical profile of normal activity on the host or network. Normal activity is measured based on volume of traffic, protocols in use, and connection patterns between
various devices. Benchmarks are established for activity based on this profile when current activity exceeds the identified boundaries an alert is generated. Weakness of this method is: it is used in environments with predictable, stable activity.

6.11 Reserve Bank of India Regulation on Business Continuity and Disaster Recovery

The Gopalkrishna Committee report includes clear recommendations and mandates on business continuity and IT disaster recovery (DR) that requires banks to demonstrate their IT recovery-readiness. Some of the important BCP/DR related mandates in the report are:

- Submit reports to the RBI on the status of recovery-readiness of critical applications and the recovery plans that banks have in place for each of these applications.
- Submit BCP/DR drill reports to the RBI. Component, subsystem, and application level testing are recommended on a quarterly and also half-yearly basis.
- Submit quarterly reports documenting major failures that critical applications have suffered and their impact on services as well as customers.

6.12 The Disaster Recovery Management

Traditional enterprise management solutions are used to keep the production systems up and efficient. This includes monitoring, performance, and routine operations on production servers and applications. DRM is the only DR-focused solution that integrates with primary and DR components, maps their relationship and co-relates events, automates the DR process, and also monitors DR health, all of which needs knowledge of primary and DR systems.
As part of solution deployment, DRM discovers the primary and DR infrastructure, including platforms, applications, and replication technologies. DRM compares discovered subsystems and their relationships against known and best-practices DR solutions, such as Oracle protection using EMC SRDF, IBM DB2 using HADR, or SAP using MaxDB. DRM offers several pre-packaged DR solution signatures that enable easy and quick deployment and DR process automation that is tested and ready to use.

In contrast, DRM automation goes through a discovery phase where all the subsystems of a DR solution, their relationships, and the dependency between the primary and DR systems are mapped. DR process automation uses the information gathered during the discovery stage to run its automation. There is a clear separation of the DR process logic that implements the recovery or drill steps and the instance of systems that it is executed on. Therefore, changing some of the subsystem information, such as the host IP address, can be automatically accommodated.

DRM goes through a discovery phase where all the subsystems of a DR solution, their relationship, and the dependency between the primary and DR systems are mapped. This information is stored in the RMDB. The DR process execution logic uses this information to sequence steps and synchronize execution of the logic. Architecturally, RMDB is implemented as an extension of CMDB.

Every supported DR solution signature in the product ships with failover workflow for application recovery and switchover and switchback workflows for DR drills.

Using these workflows ensured that the solutions deployed by the bank followed industry best practices and that recovery automation met software quality control metrics. The bank used this opportunity to review their current
solutions and processes; further custom business processes specific to the bank were easily added by extending the out-of-box workflow. DR drills are the best way to exercise a recovery plan. The big challenge in doing drills is the time and resources required to prepare for it.

Conducting DR drills is time-consuming and often peppered with moments of surprise. A better option is to replace conducting drills using run books with the DRM Drill Manager. This will enable to automate IT recovery tasks, thereby reducing drill time and resources used while dramatically improving the success rate of conducting the drills.

The DRM Drill Manager enables the automation of IT workflow. It integrates tightly with heterogeneous technologies and enables automated execution of the steps required to test various technologies. Automation is easy: and can be started with built in switchover and switch back workflow or build your own using the Recovery Automation Library (RAL), a repository of recovery steps for various technologies that can be very easily put together as a workflow. Automated workflow dramatically reduces the need for experts, reduces the time required to execute the drills, and eliminates operator errors.

Traditionally, building drill workflows requires several experts to come together and write down the required steps. Often, the execution details remain with the experts, making the test heavily people-dependent. Introducing the RAL eliminates the need for costly and error-prone scripting, drastically reduces the time taken to deploy, and increases the reliability of the drill workflow.

The life cycle approach to disaster recovery that DRM solution takes addresses the DR challenges that banks face, thereby increasing IT availability. DRM solution automates application recovery and helps banks
reduce IT downtime by recovering application within set SLAs. It addresses issues in the banking industry where the run book may be out-of-date and the steps don’t match the configuration. It also provides the bank with critical data on recovery timeframes, measured against the RTO, and the amount of data loss, measured against the RPO. More importantly, it enables banks completely automate their DR drill process, thereby saving time and resources.

**Benefits**

- DR operational efficiency, lowers the cost of DR operations, and enables agile IT organization.
- Reduce IT down time due to outages by reducing recovery times.
- Meet regulatory requirements of conducting regular drills, as automation enables faster and parallel execution of the DR drill process.
- Save time and resources required to collate data for DR reports by providing ready-made reports.
- Deploy best-practices DR solutions in the shortest time possible through packaged DR templates.

In banking industries there are various functions like providing customer service at premises providing services on alternative channels ensuring data safety, security and retrieving when required data integrity, backup Management of Technological Disasters We can call them Management of Technology in such a way so that these can be operationalize in disasters too. If one technology fails, rest can work independently or without any break. If electricity fails, UPS can work smoothly If UPS fails, Generator can work. It means there are three mode of electricity supply Main electricity.
As banks leverage IT to increase and improve their services, they face challenges in reducing business risk due to IT outages. As the number of banking applications grow, there is immense pressure on IT managers to reduce the time and resources for conducting regular ‘recovery drills’. IT managers are also mandated to gather the required documentation to demonstrate that adequate systems and processes are in place to ensure regulatory compliance.

6.13 Here are some of the key challenges that banks face:

- Disaster preparedness can be tested in an imaginary situation of disaster and managing all the activities as per the documents or plan. Every bank is now providing banking services 24x7; therefore, it is very difficult to spare time for DR drills.

- It is a big challenge for bank’s IT personnel to intervene in running IT application to test their effectiveness on disasters. Therefore, manual intervention by the technical experts is the basic requirement to test the conditions of disasters due Complex IT applications running on heterogeneous technologies.

- Managing and propagating changes that are done on the primary site to the DR site is a challenge. This can result in inconsistent application environments, causing recovery at the DR site to fail.

- The IT landscape in a bank usually consists of multiple IT applications that are interdependent and have to be accounted for when planning for recovery, such as internet banking and ATM needs core banking. These dependencies increase recovery complexity.

- IT managers have little visibility into how well their DR solutions are meeting recovery SLAs. The only time they find out about this is when they do a drill.

- Networks are more complex than ever; there are multiple layers of devices (optical/physical, Ethernet, IP) and more devices per layer.
Generally the complexity of operating a network is proportional to the number of device relationships in it, which can approach the square of the number of devices.

- The devices themselves are more complex. The number of parameters required to describe a simple interface is much larger than it was a decade ago, and there are more interfaces per device.

- Services are more complicated because they require coordinating the behavior of more devices than ever, and that means that there are more things to consider in capacity and performance management and more elements to investigate in fault management.

- Software and computer elements – part of the IT world -- are increasingly a part of the network, and these elements are not only far more complex to manage than network devices, but they introduce requirements for software updating and management, performance planning and problem troubleshooting that are totally different from those of network devices. Telecom network operations personnel normally have little experience with these new issues.

### 6.14 Business Continuity Management (BCM)

BCM is an organization-wide function comprising of a complete set of processes that identify potential threats which impact business processes in an organization. It provides a framework for building resilience for an effective response which safeguards the interests of key stake holders, reputation, brand and value creating activities. BCM ensures continuity in operation to meet legal, regulatory and contractual obligations. It is inclusive of disaster recovery, business recovery, crisis management, incident management, emergency management, contingency planning as well as alternate planning.

The BCP document for all processes may be prepared and it should be readily available to all concerned. The document requires careful planning and verification of contingency plans as these can be effective only if backup
systems are thorough, up-to-date, well-communicated and well-rehearsed. BCP encompasses *inter-alia* business, technological, human and regulatory aspects. The focus may be on prioritizing systems and processes in terms of their importance for keeping business operating smoothly and safely. To factor in changes in the processes / systems and also analyse the effectiveness of the system, a periodic audit of BCM may be done by internal / external agencies.

6.14.1 Business Continuity

Business Continuity (BC): “The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.” Keeping the business running during this time is Business Continuity.

The same approach can be taken with a system crash or when the performance of a system has degraded to the point that it has impacted business operations. So fixing the system is DR and the action of keeping the business operations running without the system being available is BC.

In conclusion, BC is all about being proactive and sustaining critical business functions whatever it takes whereas DR is the process of dealing with the aftermath and ensuring the infrastructure (system, building, etc.) is restored to the pre-interruption state.

6.14.2 Disaster Recovery

Disaster Recovery (DR): “The strategies and plans for recovering and restoring the organizations technological infrastructure and capabilities after a serious interruption. For example, the 2nd floor of a building was on fire; the fire is now out so the initial crisis is over. Now the damage caused by fire must be dealt with; there is water and smoke on the 2nd floor, the 3rd floor has damages caused by smoke and the 1st floor has water damage. The
cleanup, replacement of furniture, repair of the building and its structure, painting, plastering, etc. are all part of the disaster recovery plan. Therefore, either a system is down or a building is burnt or flooded, both should be considered a disaster and therefore both require a disaster recovery plan.

DR planning methodologies are often branded to specific consulting practices and represented as complex and convoluted processes known only to a few privileged practitioners. But in fact, the DR planning methodology is a straightforward application of common sense that follows a pragmatic project plan similar to systems development lifecycle methodology.

To do that, let us remind ourselves of the overall goals of disaster recovery planning, which are to provide strategies and procedures that can help return IT operations to an acceptable level of performance as quickly as possible following a disruptive event. The speed at which IT assets can be returned to normal or near-normal performance will impact how quickly the organization can return to business as usual or an acceptable interim state of operations.

DR doesn't have to break the bank, but depending on your organization's recovery needs, it can come with a significant investment. Frequently, these costs can be hard to justify. Many have likened DR planning to purchasing insurance, because it requires ongoing investment in something that you may never need to use.

Risk assessment is often the first step for DR and contingency planning, taking an inventory of possible risks to operations. The risk analysis involves risk identification, assessing the likelihood of the event occurring and defining the severity of the event's consequences. Risks could be anything from a power outage or hardware failure to a tornado or flood.
In this guide on risk assessments in disaster recovery planning, learn how to get started with a risk assessment, how to prepare a risk assessment, and natural versus manmade hazards in the risk assessment process.

A disaster recovery plan provides a structured approach for responding to unplanned incidents. DR plans provide step-by-step procedures for recovering disrupted systems and networks to resume normal operations. The plan identifies critical IT systems and networks, prioritizes recovery time objectives and outlines the steps needed to restart, reconfigure and recover.

Financial institutions are dependent on IT applications for running their daily operations. With disaster recovery assuming critical significance in the business world today, one of India's leading public sector banks deployed its own DR solution.

The type of DR solution chosen by the bank was driven by the outcome of the business impact analysis (BIA) it had conducted. A BIA enumerates the risks that a business could possibly face and their likely impact on the business. To mitigate the identified risks, the bank chose to deploy a three-site DR solution. Some of the key considerations for choosing the solution were:

The network delay incurred in writing a copy to the remote storage limits the distance that synchronous replication can be used for. Typically, the distance that synchronous replication can be deployed is between 60 and 100 kms. Hence, to meet the zero data loss requirement, the bank chose to have a near site. To cover the scenario in which a regional event could impact the primary site and the near site, a DR site was chosen to be in a different region of the country.
The bank has a heterogeneous environment, with the core banking application running on AIX servers, a Sybase database, and Hitachi storage and replication. The three-site data flow is setup for synchronous replication between the primary and the near site and asynchronous replication between the near site and the DR site. Other non-critical applications are configured between the primary and DR sites only. They run on Solaris servers using an Oracle database and Oracle Data Guard for replication.

Company worked closely with the bank and the System Integrator to validate the solution design before the implementation stage. The bank chose DRM as the platform to monitor and automate all the DR process for this three-site solution. DRM monitoring includes real time visibility into the health and performance of the Hitachi and Oracle Data Guard replications. Monitoring also provided real-time reports on application level RPO. A zero RPO requirement requires data to be replicated synchronously. Synchronous replication requires that when data from the server is written to storage, a copy to the local storage and a copy to the remote storage be saved on the storage before the application is able to continue.

DRM recognizes the various phases of the DR life cycle that includes data replication during normal times and the automation required to failover in times of primary outages and for conducting DR drills to test the recovery readiness of the solution.

6.14.3 Business Impact Analysis

The BIA identifies the most important business functions and the IT systems and assets that support them. Next, the risk assessment examines the internal and external threats and vulnerabilities that could negatively impact IT assets.
Disaster recovery planning is a multi-stage process, and one of the most vital of those stages is the business impact analysis (BIA). A business impact analysis is where you research the likely impact of a disruption to your organization in terms of loss of business, effects on your reputation, loss of staff and loss of data. In some ways it is the heart of the disaster recovery planning process because it is during the business impact analysis you will determine the precise effects of disaster on your organization.

Consequences of a disruption can include financial loss, reputational loss and loss of competitive position; this is in addition to potential loss of staff, loss of data and even loss of access to buildings.

BIAs are usually performed after the DR project has been launched and prior to starting risk assessments. The BIA aims to identify critical business functions and the impact of a disruption to them and provides an important starting point for defining disaster recovery strategies that are used to respond to disruptive events.

According to BS 25999, once BIAs are completed, the next step is to conduct risk assessments of the enterprise, its business units, operational infrastructure, internal and external risks and threats, and an analysis of any vulnerabilities. The BIA defines those parts of the enterprise that are deemed most critical.

The risk analysis identifies and quantifies the risks, both internal and external, that threaten the operation of critical business units and processes defined by the BIA.

Following the BIA and risk assessment, the next steps are to define, build and test detailed disaster recovery plans that can be invoked in case disaster actually strikes the organization’s critical IT assets. Such plans
provide a step-by-step process for responding to a disruptive event with steps designed to provide an easy-to-use and repeatable process for recovering damaged IT assets to normal operation as quickly as possible.

Detailed response planning and the other key parts of disaster recovery planning, such as plan maintenance, are, however, outside the scope of this article so let us get back to looking at disaster recovery risk assessment and business impact assessment in detail.

The BIA seeks to categorize and prioritize business activities for recovery, identify all internal and external dependencies associated with critical activities, determine the amount of time required to resume critical activities, and estimate the resources that each critical activity will require for resumption of business.

The BIA process is probably the longest-running and also the most critical among all business continuity activities. … The reason for this is that the discovery [is extensive] to gather relevant information about individual business units; the processes they perform; the systems and technology they use; the employees in the unit and their roles; and the unit’s relationship to other internal departments and external organizations, such as vendors and regulatory organizations.

From this information we also obtain metrics called recovery time objectives, or RTOs. RTOs … estimate the maximum amount of time the business unit and/or business function has in which to recover its systems, processes and people and then resume operations as close to normal as possible, given the circumstances of the disruption.

Another BIA activity that is often a challenge is to determine the revenue impact of a particular business function. For example, total loss of a
critical manufacturing function could result in a loss of millions of dollars in annual turnover. Other functions, such as accounting, may not have a direct relationship to revenue generation, but they’re still critical, and their value to the organization is undisputed.

Still another goal in a BIA is to identify the relationships and dependencies a business function has with other activities, both internal and external to the organization. This means defining what a critical business function needs from internal departments, such as human relations or IT, as well as external entities, such as vendors and supply chains.

6.15 Disaster recovery risk assessment

In the IT disaster recovery world, we typically focus on one or more of the following four risk scenarios, the loss of which would have a negative impact on the organization’s ability to conduct business:

- Loss of access to premises
- Loss of data
- Loss of IT function
- Loss of skills

Risk assessments focus on the risks that can lead to these outcomes.

Peter Barnes, FBCI, managing director of London-based 2C Consulting said, “The key activities from an IT risk perspective are to consider the impact on the business if delivery of critical applications and services were to be denied as a result of a fire or server failure, for example, and to assess the risks that such a scenario might arise.”

Monitors replication data lag, log apply process, current Recovery Point (for log solutions), and estimated Recovery Time DR drill Out-of-the-box workflow for switch-over and switch-back of Oracle DB, including
automation of steps for various replication technologies Recovery Out-of-the-box workflow for failover recovery of Oracle to be invoked in case of an outage Reports Standard reports on RPO, data lag, DR drill, and recovery workflow execution times.

A DR solution that is typically deployed between a primary production site and a DR site goes through various states of usage.

- Normal copy – Production is up and offering services; data is getting replicated to the DR site.
- Failover – Production sometimes goes down in an unplanned manner, causing a disruption in services. Failover is the process of bringing up the application on the DR site.
- Failback – Once the cause of the outage at the production has been fixed, primary production is ready to offer services again. The process of migrating services from the DR site back to the primary production site is referred to as failback.
- Switchover – This is part of a DR drill where production at the primary production site is brought down and the application at the DR site is brought up.
- Switchback – Once the application at the DR site has been tested, it is migrated back to the primary site and services from the primary are restored. This is referred to as a switchback.
- Run book- automation typically provides the ability to schedule and run scripts in a pre-determined sequence. The run book automation framework has no prior knowledge of the underlying topology, dependency, and current health of the subsystem on which processes are executed.
6.16 Technology Plan of Banks

Every bank has a technology plan which should be reviewed and updated periodically. Indian PSBs should move from quantitative approach to qualitative approach in IT plans. The plan should reflect banks strategies over 3 years. It commonly includes the following:

a. Overview of business strategies:
   This should contain banking goals and a specific proposed to achieve these goals.

b. Overview of the technology environment in the bank and in the industry:
   This should contain a summary of the existing technology in the bank, indicate key technology trends and any changers to the technology platform which could be needed as a result of
   1) Obsolescence of existing technology platforms
   2) The need to conform to emerging technology standards
   3) Other issues like Y2K/Euro Compliance.

c. Phone Banking

In phone banking suitable security measures for authenticating customers are available. Customer Information like account number, status are not stored in cache memory. Information shared by the customer on IVR (interactive voice response) is directly sent to the host after encryption. Information received from the host is sent back to the application when the called disconnects the call. All the information inputted by the caller is deleted automatically. From January 01, 2011, RBI has made it applicable to provide additional authentication/validation based on information not visible on cards for all on-line cards not present transactions including through IVR mode.
d. Mobile Banking

Mobile Banking is being deployed using mobile. Applications developed on one of the following channels

- SMS (Short Messaging Service)
- WAP (Wireless Access Protocol)
- Web Browser Based
- Mobile Application Client
- USSD (Unstructured Supplementary Service data is a protocol used by GSM cellular telephones to communicate with service provider’s computers)

Debit Card Security Measures

1) Personalization of card, generation of card through specific algorithm and verification of the same at switch level.
2) Delivering securely to customer after customer identification
3) Controls around activation of card
4) Blocking of cards after certain number of attempts with wrong PINs.
5) An instant SMS message is sent to the customer’s registered mobile number with the bank on usage of card at any ATM, POS (Point of Sale) or E-Commerce site.

Anti Skimming Measures

‘Card Skimming is the illegal copying of information from the magnetic strip of a credit or ATM card. This is how phishing scams are done. The scammers try to steal a customer’s details so that they can access the relative accounts. Once scammers have skimmed the card, they can create a fake or ‘cloned’ card with details from the skimmed card on it. Then he is able to run up charges on customer’s account. There are a number of methods to avoid skimming. They are as follows:
a. **Awareness**

Awareness among consumers, branch personnel and ATM service technicians can detect devices in an ATM fascia. Visual clues such as tape residue near on a card reader may indicate the former presence of a skimming device.

b. Any servicing in onsite ATMs by external service personnel should be done in the presence of a bank official. Off-site ATMs random checks should be done by the bank officials.

c. All ATMs including offsite ATMs need to be manned by security guards.

d. Physically inspecting ATM during maintenance or cash replacement by the bank or outsourced agency (which maintains ATM network for the bank)

e. Adopt visual standards for ATMs so all ATMs should look alike.

f. Banks should ask the customers to provide their mobile numbers for sending an alert message for transactions done on alternate channels.

g. Looking for anomalous activity in customer accounts. Deploying fraud monitoring system in on-line environment may be difficult and expensive but it is useful in fraud detection and timely action. Updated mobile number of the customer is critical for quick verification of fraud transaction.

h. Study of customer transaction behavioural patterns and shopping irregular transactions must be part of banks dynamics scoring models and alert transactions.

### 6.17 Data Warehousing and Data Mining

Data Warehousing means a central repository of the critical data, which help managers to take decisions, based on authentic information. Building a data warehouse is a difficult task. The type of data to be kept in data warehouse is a pivotal issue. This should be decided by banks. It
involves lengthy and tedious process of consolidating all back data from different databases.

Data warehousing at the most fundamental level is a staging area for decision support information. It collects data from various applications in an organized operational systems, integrates the data into a logical and uniform model of business subject areas. It stores the information in a manner that is accessible and understandable to all decision makers. It delivers information to all decision makers across the organizations through query and reporting tools.

It is difficult to utilize the core operational data for decision making. A warehouse overcomes this restriction by adopting a different technology/method for organization structure access of data.

2) Data ‘Populated on to a Data warehouse’.
   There are two category of data populated to a data warehouse environment. These data are defined by source
   a. Internal Data
   b. External Data

   Internal data is the data belonging to and generated by the bank. It is generated by operational transaction systems. It describes activities happening in the bank. External data may be obtained or purchased by the bank. It describes activities happening outside the bank. The purpose of analysing external data is to recognise opportunities, visualise threats and identify synergies.

IVR

Interactive voice response is a technology that allows a computer to interact with humans through the use of voice and DTMF(Dual tone multi frequency signal) tones input via keyboard.
SMS uses the popular text messaging standard to enable mobile application based banking. Advantage of deploying mobile application over SMS is almost all mobile phones, including the low end, cheaper ones which are most popular in countries like India and China are SMS enabled.

\[\text{SMS} \rightarrow \text{SMS Gateway} \rightarrow \text{SMS Centre}\]

An SMS based service is hosted on a SMS gateway that further connects to the mobile service providers SMS centre.

\[\text{Mobile Application} \rightarrow \text{WAO Gateway} \rightarrow \text{Bank’s Site}\]

WAP uses concept similar to Internet Banking. Banks maintain WAP sites accessed by customers using a WAP compatible browser on mobile phones. WAP sites offer a form based interface and can also implement security effectively. Customers can have anytime, anywhere access to a secure reliable service that allows them to access all enquiry and transactions, like trade in securities can be accessed through their phone. A WAP based service requires hosting a WAP gateway. Mobile application users access bank’s site through the WAP gateway for carrying out transactions just like internet users access a web portal to avail bank services.

**Web Browser Based**

Earlier this medium was slow and insecure. But with the launch of high end phones and browsers supporting HTML and HTTPS, it has become easy and secure. Speed of download has increased with GPRS and 3G. Its main advantage is that banks can use same infrastructure for hosting its online banking solution. It is accessible on both GSM and CDMA phones without any changes required.

**Mobile Application Client (MAC)**

Mobile Applications can be customized according to the user interface complexity supported by the mobile. They enable the implementation of a
very secure and reliable channel of communication. One requirement of MAC is that they require to be downloaded on the client device before they can be used, which further requires the mobile device to support one of the many development environments like J2ME or BREW.

J2ME has become an industry standard to deploy mobile applications and requires the mobile phone to support java language.

**USSD**

It is available only on GSM carrier networks. It can be used for many mobile banking processes such as balance inquiry, money transfer, bill payment and airtime top up. It is similar to SMS technology. It has data payload limits between 160-182 alphanumeric characters in a single transmission.

a. **GSM (Global System for Mobile Communications)**
   
   It is a standards developed by European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital Cellular networks used by mobile phones.

b. **CDMA (Code Division Multiple Access)**

   It is a digital cellular technology which uses spread spectrum techniques.

**Security Measures in Mobile Banking**

Security of financial transactions is top priority for banks. A transaction is executed from remote location and transmitted over the air. It is the most complicated challenge which has to be jointly addressed by Mobile Application Developers, Wireless Network Service Providers and the Bank. Following are the security measures with respect to mobile banking

- Security of any thick-client application running on the device. In case if the device is stolen, the hacker should require at least an ID/Password to access the application
Authentication of the device with a service provider before initiating a transaction. This should ensure that unauthorized devices are not connected to perform financial transactions.

User ID/Password authentication of bank’s customer

Two-factor authentication through mPIN or higher standard and end-to-end encryption of mPIN desirable.

The mPIN should be stored in a secure environment.

Encryption of the data being transmitted over the air

6.18 Improving the Security of Networks

Following factors should be followed for improving the security of networks

a. Inventory of authorized and unauthorized devices and software

b. Secure configuration/ hardening for all hardware and software on Laptops, Workstations, Servers and Network Devices such as Firewalls, Routers and Switches. There should be documented security baseline for all types of information systems.

c. Identify all connections to critical networks and conduct risk analysis including necessary for each connection. All unnecessary connections to critical networks should be disconnected.

d. Implementation of security features recommended by device and system vendors.

e. Establish strong controls over any medium that is used as a backdoor into the critical network.

f. Implementation of internal and external intrusion detection system, incident response system and establishing 24*7 incident monitoring.

g. Performing physical audits including vulnerabilities assessment of critical devices and networks

h. Conduct physical security surveys and assess all remote sites connected to the critical network to evaluate their security.
i. Establish critical ‘Red Teams’ to identify and evaluate possible attack scenarios.

j. Document network architecture and identify systems that server critical functions or contain sensitive information that require additional levels of protection.

k. Establish a rigorous, ongoing risk management process.

l. Establish a network protection strategy. Layered security based on principle of defence-in-depth. It requires suitable measures to address vulnerabilities across the hardware, operating system, middleware, database, network and application layers. It is necessary for banks. To protect against insider threat, restrict users to access only those resources necessary to perform their job functions.

m. Disaster recovery plan should allow rapid recovery from any emergency including cyber attacks.

n. Establish policies and conduct training to minimize the chances of disclosure of bank’s sensitive regarding Critical System Design, Operations and Security Controls through Social Engineering attempts. Any request for information by unknown persons need to be sent to a central network security location for verification and fulfilment.

o. Network control functions should be performed by individuals processing adequate training and experience. Network control functions should be separated and duties should be rotated on a regular basis. Network control software must restrict operator access to perform certain functions like ability to amend/delete operator activity logs.

p. Network control software should maintain an audit trait of all operator activities. Audit trail should be reviewed periodically by operations management to detect any unauthorized network operations activities.

q. Network operations standards and protocols should be documented and should be reviewed periodically by the operators.
r. Network access by system engineers should be monitored and reviewed closely to detect unauthorized access to the network.

s. Users should be identified at every step of their activities.

6.19 **Structure of data Warehouse**

Data warehouse has a distinct structure. It has different levels of summarisation and details that demarcate the data warehouse. Different components of data warehouse are Meta Data, Current Detail Data, Older Detail Data and Summarised Data. Metadata can be classified as follows :-

- Technical metadata
- Information about data resources
- Warehouse object and data structure definitions
- Rules to perform data cleanup and data enhancement
- Data mapping
- Access metadata
- Business metadata
- Subject areas and information object type
- Internet home pages
- Other information to support all data warehousing components
- Data warehouse operational information

The Current Detailed Data is major concern because it reflects the most recent happenings and always stored on a disc which is easy to access by anyone.

The Older Detail Data is the Data that is frequently accessed and stored at a level of detail consistent with current detail data. The storage medium of Older Data is usually removable storage such as automatic tape library. This is because large volume of data is coupled with infrequent access of data.
The Summarized data is of two types, according to the processing and storage.

**Figure 6.1 Summarized data**

Lightly summarized is data that is distilled from the current detailed level. This level of data warehouse is always stored on disc storage. Highly summarized is compact and easily accessible.

**Access Tools**

Following are the front end tools for user interaction. They support both dynamic and pre-planned analysis. They use metadata for accessing the warehouse. They can be classified in five main groups: - Data query and Reporting Tools, Application Development Tools, Executive Information Systems Tools, Online Analytical Processing Tools and Data Mining Tools.

Online Analytical Application (OLAP)

Data Warehouse uses ‘Multi Dimensional Data Basis (MDDB)’ architecture. It can be implemented using relational technology with stars schema. It has to solve complex queries.

MDDB recites in spread sheets, relational database or legacy data managers. The data access and analysis tools must be able to take enterprise data from a variety of sources and give work groups the accessibility, power
and flexibility. Only multi dimensional analysis provides a clear picture of bank at any given time.

**Characteristics of OLAP**

- The ability to scale large volume of data and large number of concurrent users.
- Provides fast interactive response time.
- Provides for analysis time series.
- Supports ‘what IF’ analysis and planning in a multiuser read write environment.
- Robust data access security and user management.
- Availability of a wide variety of viewing and analysis tools and support different community.

**Data Mining**

Data Mining is the process of extracting hidden information from databases. The need of data mining aroused from handling large databases (data warehouse) and storing customer information.

**Features**

It helps in predicting futures trends and behaviour allowing banks to make proactive and knowledge driven decisions. It is viewed as corollary to data warehousing because of the necessity to integrate and derive new information that transactional systems do not provide. It also allows building the data mountain. Shifting the mountain down to the level of essential information that is useful to the bank.

‘Some nuggets of gold hidden in the mountain of data and Data Mining can find the gold which would otherwise be too costly or too difficult to find without Data Mining Tools.’
Data Mining Techniques

1. Classifications – This technique is used to classify database records into a number of redefine classes based on certain criteria. Example:- A bank wants to classify its customer’s records as good, medium or poor risk based on the attributes income and age. The generated value could be that a customer in the age of group between 50-60 within income greater than Rs. 50,000 have good credit risk.

2. Clustering and Segmentation – This technique is used to segment the database into different clusters based on a set of attributes. Records with the same attributes are in the same cluster.

3. Association Rules - These techniques are often used for market basket analysis and discover rules that are hidden between the attributes.

4. Sequencing – This technique helps in identifying patterns in times series. This is useful for stock market predictions or for catalogue companies. Example – Companies might discover that buyers of today buy learning software for children five years later.

5. Decision Tree – It is a predictive model that can be perceived as a tree. Each branch of the tree is a classification question and the leaves are the partitions with their classifications.

6. Natural Networks – This technique try to stimulate the human brain. The nodes of the natural networks are connected and every connection has a weight.

7. Training Output - Output = Error-The difference between the Output and the Training Output is called Error. The weights are adjusted according to the error. Natural networks can handle noise in the data and are good for most of the problems but it cannot analyse knowledge like decision trees.

8. Genetic Algorithms – These algorithms stimulate the biological evolution. The attributes are coded like the DNA a lot of individuals
are generated and from generation to generation they change their DNA with operations like *Mutation and Cross over*. The survival of the fittest principals select only individuals that are better than the generation before.

9. **Rule Induction (Association Rules)** – In this technique all possible patterns in the database are systematically pulled-out and then the accuracy and the coverage are calculated. The rules are easy to understand.

### 6.2 Disaster Management in Selected Banks

#### 6.2.1 Punjab National Bank

Banks’ data centre and Disaster Recovery Site (DRS) offers hosted services for all overseas ventures, including Joint Ventures and subsidiaries. The data centre manages operations of 13 entities with ‘In House’ resources as against outsourced model thereby reducing the operational costs considerably and affording complete control over operations.

The effectiveness of the channel is enhanced with the utility payment facility for all the popular service providers SMS Alert facility is being availed by over 21 lac customers through generation of SMS Alerts on identified financial transactions undertaken through branches and delivery channels (POS, ATM, Internet Banking and Mobile Banking).

The SMS Alerts are being sent for certain non-financial activities as well. The channel was leveraged for providing information on Bank’s products and services over SMS under the SMS Pull Mechanism.

**Business Continuity Plan (BCP)**

In the present scenario where all the branches are under Centralized Network connectivity is an important concern. Though precautions have been taken to take care of connectivity outage by providing dual connectivity to
each branch, yet chances of outage cannot be ruled out completely. Bank has well defined Business Continuity Plan (BCP) to provide uninterrupted customer Service in case of any exigency in the branches.

The Bank has taken adequate steps to strengthen anti-phishing mechanism and monitoring process thereof to prevent online frauds. To monitor information security events across Bank’s network, a world class Security Operations Centre (SOC) has been established being first of its kind to be set up by any Indian Bank. The facility is being utilized for analysis and monitoring of various threats emanating from both within the network as well as from outside the network in a very proactive manner.

Bank’s Critical Infrastructure Data Centre, Network Operation Centre & Disaster Recovery Data Site are ISO 27001 certified. All the policies are aligned with best practices and are ISO 27001 standards compliant.

**Daily malware monitoring of the official websites.**

To safeguard the interests of our internet banking customers, Anti-Phishing, Anti Pharming and anti -Trojan services are being availed.

To secure the interests of Internet banking customers, ‘Site to user functionality of transaction Monitoring solution (IBS Shield)’ has been implemented.

Banks have adopted IT in a big way in order to provide better service to the large customer base of the individual banks. The general awareness on the IT risks and its effects are yet to catch up the importance in banking industry and hence, the perils due to IT risk management, exist.

The focus of IT Security programme is to enlighten the nature of IT risks associated in every face of IT deployment and its safeguarding methodologies. Its further emphasis is on IT act, security policy issues,
Disaster recovery and BCP and to protect the electronic form of exchanges and processing. Its ultimate objective is to make people aware about possible threats of IT and its protective measures.

6.2.2 UCO Bank

UCO Bank has outsourced its security Disaster strategy to Xchanging. Xchanging is IT Company which has extended its relationship with UCO Bank, a leading Indian bank, to implement mission critical disaster recovery solution for its most business critical financial telecommunication infrastructure which has given the centrality of IT to all major business operations, putting in place a business continuity planning strategy with a focus on IT disaster recovery management.

Exchanging will enable UCO Bank to seamlessly integrate near real-time databases, payments, and transactions over its SWIFT payment gateway with the bank’s existing disaster recovery infrastructure. Exchanging EastNets’ implementation compliance and payment solution conforms to international banking benchmarks. The solution will provide a secure environment for efficient duplication detection, and recoverability of high volume messaging traffic. The scope of the implementation also includes back-up of foreign exchange payments and telecommunications platform. Exchanging’s comprehensive disaster recovery solution will address the data recovery needs of the bank’s operations.

Exchanging has been supporting UCO Bank since 2004 as a SWIFT Partner. Exchanging’s mission critical solution will allow UCO Bank to streamline its back-up and recovery practices and derive increased operational efficiencies.

In the event of any hardware failure, human error, file system corruption or disaster, our solution will help the bank to restart operations.
without any delay in switching to the back-up system”. He further added, “We are seeing a growing number of banks adopt an increasingly focused approach towards disaster recovery management planning. This is spurred by an increased regulatory thrust by the Reserve Bank of India (RBI). UCO Bank when looking for a strategic partner to augment its disaster recovery planning selected Exchanging after a careful assessment of the depth of our experience”.

6.2.3 Bank of Baroda

Moreover, your Bank undertook measures to create Data Warehouse for providing flexible and interactive source of strategic information, Customer Relationship Management for better customer insight and uniform customer view across channels.

Bank’s IT-enabled Business Transformation Programme:

- Bank has built and commissioned its own State-of-the-Art Global Data Centre (DC) for running its centralized banking solution and other applications in 3176 branches across India and 21 other counties where the Bank is operating. The Data Centre will function as a central data hub of the Bank for both its domestic and international operations. It conforms to critical technology standards and is equipped with full Communication and network infrastructure, meeting all the attributes of a Tier III Data Centre.

- Disaster Recovery Site (DRS) which is a replica of Data centre has also been fully operationalized.

- Bank is shortly setting up “Near Data Centre” for online “near real time” replication of data to avoid any data loss.

- Bank of Baroda has put in place robust Information Security Management System to ensure confidentiality, integrity, and availability of its IT resources. Multi-layered security architecture has
been implemented with firewalls, NIPS, HIPS, regular patch updating anti-virus & anti-spyware, centralized domain controlling, application security, database security, physical & logical access control measures etc.

- Bank has an updated IT Security Policy, standards and guidelines, which have been formulated to address the evolving threat landscape and Bank’s endeavor to provide safe technology enabled services to its customers.

- For internet banking, 128-bit VeriSign SSL certificate has been implemented to ensure that customers’ data is transmitted in encrypted form over internet. To prevent fraudulent fund transfers, mandatory beneficiary registration has been implemented for third party fund transfers in internet banking.

- Bank’s IT assets are subjected to periodical audits, vulnerability assessment and penetration testing to assess the vulnerabilities / risks and implement necessary risk mitigation measures.

6.2.4 State Bank of India

- SBI provides a process to manage the availability of the applications, database, systems and hardware.

- SBI delivers a process to recover from a disaster in a predictable time with applications and data synchronized.

- SBI has a process to guarantee that from the time a security patch is available from R&D it is applied to the production systems in a known period of time.

- SBI delivers a process to insure that an independent audit is performed at least once a year.

- SBI provides a process to escalate problems to resolution.

- SBI provides a process to take high priority fixes from the development team and apply them in a predictable amount of time.
SBI provides a process to insure, on a periodic basis, there are adequate hardware and software resources to deliver a specified level of application performance.

SBI has a process to add and shed infrastructure (computers & people) as load increases and decreases.

Managed and maintained to industry standards

Certified configurations with integration throughout the entire technology stack

Third party applications part of certified configurations

Defined solid Change Control Policies

Created solid Configuration Management

Dedicated experts available 24/7 by 365 to resolve and proactively identify service interruption.