



**Several banks are quietly upgrading and consolidating their disaster recovery processes. Executive editor N. Mohan meets some of the IT heads of banks to get an insight into their thinking:**

**S**uccessful and professionally run enterprises anticipate disasters and address them proactively. In an IT environment, a disaster can cause extreme downtime, total interruption of processes and breakdown of communication channels causing disruption in business operations, loss of revenue, higher expenses and reputational loss. An effective disaster recovery planning and consequence management can offer many benefits to a business. Once the value of technology to an organization is acknowledged, the related consequences, when and if that technology ceases to be temporarily unavailable, also need to be considered.

Experts recommend a three-pronged DR strategy for any IT-driven organization: (i) prevention, which can totally avoid or minimize occurrence of disasters, (ii) anticipation, in which likely disaster scenarios can be identified and preventive action taken and (iii) mitigation in which corrective steps can be initiated at the right time to minimize the impact of disasters.

It is gratifying to know that banking industry in India is very conscious of having efficient DR setups and costs are not a major concern. Many banks have 100% replicated remote DR sites, automated protocols and processes and dedicated trained staff.

Emphasizing the need to situate technology risk identification in the overall business strategy of an institution, Sanjay Sharma, managing director, IDBI Intech, the technology arm of IDBI Bank, says the 9/11 bombing of the World Trade Center showed the importance and utility of disaster planning measures, as seen in the fact that a huge majority of information systems emerged

relatively unscathed and were fully recovered. "However, it is also true that continuity in key business processes was greatly at risk because of significant gaps," says he, adding, "it cannot be overemphasized: technology risks are closely interwoven with the institutional fabric, and to manage them effectively they must be examined from the perspective of the whole institution."

He explains disaster management thus: "Disaster management involves: (i) pre-disaster planning, preparedness, monitoring including relief management capability, (ii) prediction and early warning, and (iii) damage assessment and relief management."

He says disaster recovery is of particular importance for banks in a locality hit by crisis - more so than other businesses - because their services are in great demand during times of community disaster. "Disaster recovery plans should take into consideration any outsourced functions. The final component of a successful recovery planning effort is testing. Disaster recovery will continue to evolve with the banking industry. As banks become more sophisticated technology users, disaster recovery solutions will follow."

### **DR PREPAREDNESS**

What is the DR-preparedness of some of the leading banks? How do DR managers look at DR as a function?

Says Patrick Kishore, GM & CISO, State Bank of India: "When we started induction of information technology in the bank, we had taken a conscious decision to have a disaster recovery site which will be an exact identical set-up to that of the primary site but situated at another city in a different seismic zone. Today, the DR site is a replication of our primary center, which hosts all the applications. This ensures that in the case of an eventuality, no data is lost and we can resume our normal operations with a minimum downtime. In terms of the criticality and volume of our operations and in order to ensure nil data loss because of any downtime, we have also set up a near site, which is within a distance of 20 to 30 kms from our primary site."

He adds: "We had a disaster-like situation on 26 July 2005, when the entire Mumbai and Navi Mumbai were flooded. Flood waters entered the basement of our global IT center in

Belapur and as the situation grew worse, our DR team decided to shut down the center as we feared that the power supply could come to a halt, and to activate the DR site. The first to be shut down was the ATM switch, and within half-an-hour the switch started functioning from the DR center. The team then started activating the other applications from the DR center. Yes, there was some downtime as far as the other applications were concerned, but it was not noticed by our customers. Next day morning, we got pumps to get the water in the basement pumped out and the primary site started functioning. While all other applications were reactivated at the primary site on the next day of the flooding, we brought back the ATM switch after a gap of three to four days as we did not want to take a chance.”



Patrick Kishore



Subhakanta Satpathy

In a scenario where the primary center itself is damaged, the bank has devised a system of relocating the work area. This site is situated in a nearby city, which can be accessed by road in a short time. There are desk top systems at this center which are configured to work as terminals at the primary site and the staff rushes to this center and takes over. In short, the primary work site in Mumbai is replicated at this site. The advantage is that the down time can be reduced to the extent possible.

### THREE-LAYERED SETUP

Barclays Bank, which came into India in November 2006 as a day zero set up, has a DR set up, which is three-layered, consisting of a primary site, a near city site and a remote DR site. Says Sridhar Guru, director – Information Technology, Barclays GRCB: “As much as 80% of all the applications are replicated, which provides 100% coverage to business continuity and disaster requirements. As far as critical applications are concerned, they are hosted at the three sites. I must emphasize that ‘capacitization’ of the DR site is an ongoing exercise and in our case, we look ahead five years from now as far as technology platform is concerned. To this extent, we are DR-prepared in the truest sense of the term. From the operations/business side, there is a well tested business continuity plan in place, even though this is outside of the information technology ambit. However, the two work hand in hand and add to the comfort levels of the organization.”

Private sector Axis Bank has a system of storage box level mirroring and database servers on clusters in its primary setup. “We do not maintain a separate near DR site as our experience has shown that the existing system is adequate,” says Subhakanta Satpathy, Sr VP - IT, of the bank. “In case of a failure of the database server, the fallback database server can take over and the database will not crash. There is a fully replicated DR site at a remote location, which is capable of taking over the entire operations in case there is a disaster at the primary site. Using Dataguard utility we replicate the production set up at the DR site. Our DR site is of the same capacity as of the primary.”

Satpathy says in the unlikely event of both the file systems (primary and secondary storage at production site) becoming unstable and not available, the data loss will be to the extent of the last log file under production (and last log file under

transmission). The bank can handle this eventuality in two ways: (i) identifying the last transaction time stamp and advise branches to recreate the lost transactions from journal/vouchers. (Detailed procedure has been drawn up to handle the recreation of lost transactions accurately); and (ii) recreating the lost channel transactions in core banking through a tool, which extracts the same from multiple channels like ATM and e-banking.

HDFC Bank too has a DR structure that is three-layered - a primary site, which hosts all the applications, a near site, which is a replication of the primary site, and a remote DR site, which again is a 100% replication of the primary site. Says Deepak Mudalgikar, VP - IT, of the bank: “The whole plan revolves around a basic risk impact, vulnerability impact and business impact. The plan is well documented with roles and responsibilities meticulously defined. The plan helps the business to make optimum use of information technology.”

### IT-BCP PROGRAM

Mudalgikar outlines the genesis and the current status of the DR setup in the bank: “The bank started working on System DRP in 2002. The objective was to ensure that business can recover and resume services with minimal to no data loss, after a failure / disaster. As part of this project, we had implemented DR setup at Chennai for identified eight core banking mission critical applications. In 2006, we initiated the IT-BCP program, which broadly aimed at (i) providing a DR solution for each and every application, (ii) setting up and documenting in adherence BCP framework, COBIT and RBI guidelines, (iii) setting up an automated switch over, switch back, fail over and fall back process, (iv) preparing the runbooks for these application and undertaking periodic reviews of them, (v) carrying out periodic drills for the BCP ready applications, (vi) ensuring seamless connectivity to the BCP setup for users, and (vii) online monitoring of RPO & RTO and integration with an enterprise monitoring system. To achieve network redundancy, DR datacenter is connected to primary datacenter via 2 STM4 links (600 Mbps each). In the second phase, more than 40 critical applications that were identified through a business impact analysis were brought under the BCP umbrella. These applications are hosted across four different data centers in Mumbai. We intend to take up at least 30 more applications in the next phase of the BCP project. The BCP framework involves carrying out and documenting business impact analysis, risk assessment and current state assessment of each of the applications. We again ensured that this complies to COBIT framework and RBI guidelines.”

The salient feature of the complete DR solution is that it is user agnostic and supports partial failover. “Users’ connections are seamlessly diverted to the application at DR site, once failed over. Mind you, more than 30,000 employees are accessing the various applications at any given point of time. While the bank has setup BCP for more than 48 applications, the solution provided helps us in invoking BCP for any one or multiple applications. This, we have termed as partial failover. During such scenarios,

all the interfaces between all the applications continue to work, irrespective of the location they are hosted, involving no manual intervention," says Mudalgikar.

Another private bank, the Federal Bank, has not lagged behind. In earlier days the bank had a remote DR site in a hosted environment. The thinking at that time was to economize and avoid unnecessary expenses as disaster recovery as a concept had the least preference and for bankers it was a last resort. "However, this thinking changed in the last two years and we decided to have a DR site with 100% capacity had have it located in our own setup, but at a remote location," says Rajagopal Nair, GM – IT, of the bank. "At present, we are in the process of commissioning the hardware and software and deploying automated tools. This work is in the late stages of completion and in a short period of time, we will have 100% redundancy at the DR site. We are also evaluating DR automation tools like those offered by Sanovi Technologies (India), to make our DR framework efficient and fully automated and cut down on RTO and RPO. When fully commissioned, we will have a four-layered system - the primary site, located at our head office in Alwaye, Kerala, which has the database, application, production and other servers; the remote DR site, which when fully upgraded, will provide 100% redundancy and will ensure automatic switchover in case of an eventuality; a command center, which will be in another building and which will again be a facility that will help us activate the DR center in case of a major eventuality that will render our primary site inoperable; and a near site, which in effect, is an intermediate layer of data security and will function synchronously with the primary centre, capturing, on a real-time basis, all customer transactions at branches and ATMs. We believe such an architecture will help us avoid exigencies like floods which could effectively shut down the primary site with no means to activate the DR site."

## MOCK DRILLS

Mock drills are one way to assess the DR readiness of a bank. Patrick Kishore says State Bank of India conducts a DR drill every six months in real life conditions. "These drills constitute integrated testing of our DR preparedness and cover State Bank of India and its seven associate banks. It amounts to a graceful shutdown of our data center with an emergency DR team taking over and the DR site getting activated. It's business as usual without even the other staff members ever coming to know that the drill is on. We did such a drill in June 2009 and within three to six minutes of the graceful shut down of the primary site, the DR team took over the entire system administration and processing and it was smooth continuity of the business."

At the time of the June 2009 drill, which was a global drill where all the branches of the bank and the associate banks situated in India and abroad were covered, the IT team actually enacted a situation when the DR team traveled up to the remote center where the primary site is replicated and activated the system there and started interacting with the DR site staff.

Satpathy of Axis Bank too says the drills are routine. "We



Sridhar Guru



Deepak Mudalgikar

undertake drills at specific intervals to test our DR readiness as far as the core systems are concerned. We never had any major crisis that affected our operations in a major way. The flooding that halted activities in Mumbai in 2006 had been an experience for the bank. We managed to operate from our production site in an uninterrupted manner for the entire crisis period. We used the experience to test and validate our internal processes meaningfully."

Barclays Bank carries out DR readiness drills every quarter. In fact, this is a combined exercise run by the BCP and DR teams. These drills demonstrate the readiness of the bank's technology team to meet any eventuality. Most of the time, such drills are not known to the users of the systems. "For example," says Guru, "during the 26 November 2008 terrorist attacks in Mumbai, while we did not invoke our DR, we got the resilience of our primary systems tested. The second occasion, more recently, was when the swine flu epidemic affected various parts of the country."

HDFC Bank has defined five stages to achieve a BCP readiness for each application. Each stage is a drill in itself, says Mudalgikar, "with the last stage as the live drill for the application with all the users accessing the setup at the DR site. Successful completion of this stage marks application as BCP ready. In the last one year, more than 70 DR drills at various levels were conducted to make all the applications DR ready. In addition, there are periodic DR drills conducted for all the BCP ready applications."

He adds that the roles and responsibilities of staff concerned with handling disaster are well defined. Once a decision is taken by the crisis management team, the DR team at the remote site takes over. "We have 60:40 ratio of our datacenter staff and support staff, 60% staff at production and 40% at the DR site."

He says there has been no instance of activating the DR site. The bank all along has been able to manage with the local standby. However, it has switched applications to the DR site as part of the DR drills and this has been quite successful.

"The comeback from a DR site is time consuming and hence activation of DR site is the last resort. What I can do is to make use of the local standby setup in case of a partial failure in active/passive mode. At the end of the day, the objective is high availability of the applications either from the primary site or the DR site. The decision is taken on the basis of the nature of breakdown," says he.

## RTO, RPO

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are two key metrics mapped into the IT infrastructure in an organization's BCP/DR. The banks are keen that their RTO/RPO is at the minimum levels. Patrick Kishore says State Bank of India and its associate banks have set a RTO of three hours and a zero RPO. This is made possible with the near site.

According to Mudalgikar, the RPO and RTO vary from application to application. In any case, he says HDFC Bank has been able to maintain RPO within a range of zero minutes to five minutes. "We should be able to scale this down to virtually zero in the days to come when we will be able to strengthen our applications to ensure assured data availability."

## Fundamentals of a Successful DR Plan

Any effective disaster recovery preparations can be costly, time consuming, and technically challenging. A successful business continuity/DR plan will have two critical core components - a setup to manage replication processes and sound connectivity. Two main metrics used in measuring the success of a BC/DR plan are recovery point objectives (RPO) and recovery time objectives (RTO), which measure the amount of data lost during a disaster and the time required to restore to normal operations. IT managers strive to have the lowest RTO and RPO possible even as they grapple with issues like increased data storage requirements as a result of increased usage and regulatory archival requirements, constraints of bandwidth between primary and backup locations and factors that can affect the performance of the DR solution over the WAN.

In order to minimize the impact such an undertaking would have on scarce resources, the project for the development and implementation of disaster recovery and business resumption plans should be part of the organization's normal planning activities. Enterprises today invest not only in backup and recovery protection but also in replication, mirroring and failover technologies. All these require a rugged system of testing, which is a complex issue. And add to these the issue of replicating primary system changes on to the secondary system, and be assured the DR environment is prone to failure.

For financial services institutions, the most fundamental aspects for evolving a successful DR program are:

1. Executive management level visibility and involvement. It is only when executive management is involved, will adequate resources and priorities be assigned to getting IT DR ready and working.
2. Create a DR plan, assign a resource to keep it up to date. This is the first and foremost step in having a DR plan. Hoping that the IT team will figure it out at the time of crisis will not work. Choosing a data replication technology is not DR, it is only a prelude to what is required to have a DR that works.
3. Test the DR plan. This is a bitter pill that is a must. Every IT team must make time and resources to test its plan at regular interval. Otherwise there is no confirmation that the DR plan is of use.

Once a DR plan is in place, IT team can take several steps to

successfully operationalize the plan and make sure that the DR technology delivers to meet business expectations. These can be listed as:

1. Ensure visibility. Monitoring the DR solution is the best way to find out if it is meeting recovery objectives.
2. Reduce dependency on people. In a crisis, people working under pressure jeopardizes IT recovery. The steps to recovery must be well documented and automated so that operator error is eliminated and the right person being there is ensured.
3. Test the DR solution. It is necessary to put in place processes and technology to reduce time and people required to do DR drills. Verification of pre-requisites and automation of drill steps can dramatically reduce the time and dependence on experts. This enables doing drills at more frequent intervals, which gives IT the confidences that application recovery will work when required.

### Trends in Disaster Recovery

What was once thought of as an insurance policy is now turning out to be a strategic differentiator. As business dependence on IT increases, application uptime is of utmost importance. An agile IT with the confidence to recover applications can deliver just that. DR Management is an emerging area that offers a comprehensive view of DR and recovery readiness. DR Management provides the visibility that business needs into recovery readiness and process automation that IT can rely on to make recovery predictable. Organizations are deploying DR solutions with a focus on predictable recovery that can be invoked when critical applications go down irrespective of the cause, may it be an act of God or infrastructure/operator failure.

Says Chandrasekhar Pulmarasetti, chief technology officer of Sanovi Technologies, a leading provider of DR management solutions to enterprises: "Businesses lack a single dashboard that gives them a real time view on their recovery readiness of critical applications. DR Management provides the tools to monitor recovery metrics and the capability to automate DR process and provide a dashboard view to ensure compliance to regulators and auditors."



Satpathy says for Axis Bank the RTO for the core applications like CBS is less than one hour in a planned switch over mode.

For Barclays Bank, the parameters are well within the prescribed limits and Guru says the bank can overcome any eventuality within the shortest time frame. "In fact, there is a central coordinating team which handles the situation in case of any eventuality and the brief given to this team is to ensure that we get back on track with the minimum of downtime."

Nair of Federal Bank says at present the bank has an RTO of four hours and an RPO of 15 minutes. "Once we induct the automated DR management system, the RTO is bound to come down to less than an hour and RPO just about five minutes," he avers.

### EXECUTIVE LEVEL VISIBILITY

What about executive level visibility for DR systems? The bankers say this is relevant and highly required. Management involvement is a must to have effective system in place. Guru gives an outline of how this happens in Barclays: "This is at three levels, the first line of defense, second line of defense and third line of defense. Any functionary in the bank is expected to know the procedures to be followed in case of a disaster. The responsibilities of each colleagues is clearly defined in terms of the role that he / she is expected to play. In the first line of defense, there are people designated to handle BCP/DR in case of an eventuality and it is

their responsibility to react and bring the situation under control. In the second line of defense, there is a central core team which is responsible for all the systems to be functional and ensure that the bank is DR-ready. The team comprises both technology and business people. The third line of defense is basically an internal auditor, who is mandated to carry out an audit of the BCP/DR functions prevailing at Barclays and report his / her findings to a committee of the Board of Barclays Plc in the UK. This is a full time assignment and the concerned colleague is empowered to recommend various measures to ensure success of the BCP/DR. The board committee monitors the BCP/DR function periodically based on the report of the audit team."

## INVESTMENTS IN DR

Do investments in DR infrastructure offer the right RoI? Views vary.

Mudalgikar says it is like an insurance policy. "We have made huge investment to the tune of nearly Rs 100 crore in our DR site. We have replicated applications and setups and have dedicated personnel for these setups. In addition to this, we have ensured that each and every back office operations unit is located at multiple locations across India. We are a customer-centric bank and even a minute's downtime is intolerable. So the investment in DR setup is totally justified."

Satpathy of Axis Bank says the investments in DR systems do not really pay off. "It's an insurance essential for any financial entity serving large customer base and is also a regulatory requirement. However, we do utilize the DR site resources to run data mining and business analytics to bring about some level of efficiency."

For Patrick Kishore, the huge investment the bank has done in DR systems is quite justified. He cites the reasons: "As a public sector bank and as the No 1 bank in the country, we are critical to the country's economy. In fact, a very large part of the country's economy passes through us, whether it is market funds or government funds. Again, a sizeable chunk of foreign inward and outward remittances are passing through us. As such, it is imperative for us to have a strong IT infrastructure and we have not compromised on anything. Especially in having a full-fledged and effective DR setup. For that matter, we do not compromise on anything that concerns information technology induction. We ensure that there is enough redundancy built in whether it is servers or whether it is connectivity, even though there is a tremendous cost pressure. This ensures little or no downtime in our operations."

State Bank of India when it started setting up its near site in 2004-05, had engaged a consultant, Sanovi Technologies (India), a firm that assists enterprises like banks to proactively manage DR systems through its DR management software solutions. "The association had been quite helpful and advantageous," says Patrick Kishore. "The firm advised us to have dark fiber connectivity between our primary site and the near site. As you know, having a dark fiber is very advantageous as it ensures that there is no delay or latency in updating the servers and in realtime. However, the connectivity costs are quite high, but it is worth the cost, as being a bank we cannot afford to have any data loss in a disaster."

## CERTIFICATIONS

The bank is also planning to obtain international certification for its business continuity plan. "We are planning to obtain BS 25999, a certification from the Business Continuity Management

Institute. The certification specifies the requirements for implementing, operating and improving a documented Business Continuity Management System (BCMS). It is a certification that our processes, systems and people are mature and capable of implementing BCMS. We intend to have the certification next year," says Patrick Kishore.

While HDFC Bank has not gone in for any certifications, its processes, systems and people are very much in sync. The bank is very aggressive about its business continuity planning. There is a BCP manager, who has unique exposure to business, technology and security. There are periodic steering committee meetings of group heads of business, technology and operations to review BCP and upgrade the systems if required in terms of systems risks and transactions risks. This is a continuous process. In addition, the bank also carries out internal IT audit to ensure that the systems are fine-tuned and DR-ready. The bank also adheres to the COBIT and RBI guidelines, which in itself are tantamount to certifications.

Axis Bank has also not opted for any certifications. But, says Satpathy, IT systems, processes and support people are very much in place. "We shall go in for certifications in future."

Guru of Barclays sums up the importance that the bank gives to systems and procedures. "Security, resilience and risk management are non-negotiable dictates for us in building and running the technology proposition for the business. Systems are further classified based on priority to business and operations, with a view to offer the most efficient, cost-effective and continuous services to customers. We involve the business and operations leaders in all facets of resilience and risk management - conceptualization, prioritization, planning and execution. All our investments in technology, including technology for DR/BCP, are in line with our business requirements. It is dependent on the payback we receive in our operations. We have an efficient risk management practice in place. Risks are mapped in terms of business needs and the management of these risks are structured on the specific condition that prevails in India. We have evolved a unique risk practice for our operations in the country, encompassing the entire life cycle, that is, from software acquisition, product development, service transition and service delivery. We also evaluate asset risk at various levels - in terms of quantity and quality."

[mohan@bankingfrontiers.com](mailto:mohan@bankingfrontiers.com)



## BSNL to set up IDCs

Bharat Sanchar Nigam (BSNL) is planning to set up and operate internet data centers in the country on a revenue-sharing model. The telecom behemoth has sought initial bids from information technology companies for this purpose. It plans to have IDCs in cities including Jaipur, Ahmedabad, Mumbai, Faridabad, Ghaziabad, Ludhiana, Hyderabad, Ernakulam, Bangalore and Ranchi. The successful bidders will have to incur the capital expenditure on hardware and software while BSNL will provide the space to set up the centers.