News

BCP/DR: your safety net

Ashwani Mishra
18 August 2009 00:00 am

Business continuity planning and disaster recovery are essential for an organisation's very survival—and planning for contingencies can be a high-risk tightrope

Circus acts are thrilling, aren't they? Wild, awe-inspiring and at times mysterious. The performers test the limits of human physicality, of the human body. They repeatedly test outer limits as they strive to surpass them, especially trapeze artists.

Most of us have watched these artists perform their stunts—swinging on the trapeze, somersaulting and flying through the air, performing catch-and-release moves. We just cannot take our eyes off their performance and sit completely engrossed. But we miss something. A thing that these artists are aware at all times the safety net placed below.

The direct purpose is to protect falling acrobats by having the net catch them before they can harm themselves and traumatise the audience by splattering against the ground.

Granted, that a circus cannot be compared to the high stakes involved with enterprise and government businesses, however, the business safety net shares many metaphorical entailments with its circus counterpart.

First, like acrobats, businesses may choose to engage in risky activities that critical mistakes can quickly cripple them or even end their existence. Second, just as circus managers, business regulators or auditors or compliance framework guardians must plan and shield against any risks associated with the business and produce benefits just like the safety net does.

Always open for business

Disasters happen. Be it a weather phenomenon or something much more sinister, disasters can creep into a company and sap its livelihood. Post the Mumbai terror attacks on November 26, 2008, Business Continuity Planning and Disaster Recovery (BCP/DR) have become a key priority within enterprise circles. Taking the element of surprise out of a disaster, natural or otherwise, is exactly what a BCP/DR is all about.

"BCP and DR are two different things. BCP by itself covers the entire spectrum of the business cycle or touch points within an organisation. It revolves around people and processes. DR is the technology piece and is a subset of BCP. In these times, there is a strong need for enterprises to have a robust BCP/DR plan in place that is tested on a continuous basis to handle disasters of all kinds and minimise any negative impact on the employees and the bottom line," says K M Asawa, DGM, Projects and IT Infrastructure, Bank of Baroda.

Take the example of the recently concluded two-day G-20 summit in London. Majority of the financial institutions were prepared for any disruptions by anti-capitalists, environmentalists as well as terror attacks. The G-20 is a group of finance ministers and central bank governors from 20 countries and the European Union (EU).

According to reports, the IT operations of these firms enabled remote working. Most of the IT was hosted in secure

datacentres with IT staff able to access systems from other locations. The institutions directed their staff to multiple offices where they based themselves and were ready for any business disruption.

"Enterprises need to identify the risks, carry out a business impact analysis—like what business applications are the most critical and where do they stand in terms of BCP/DR at present. The other crucial task is to work out the timeframe in which they can get back to normalcy," says Atul Hemani, Managing Director, Omnitech Infosolutions.

According to Hemani, the BCP/DR strategy involves looking at four key aspects. These are data, IT equipment, a DR site and people. He opines that to safeguard the lives of employees should be the first step in a BCP plan. Once this is done, enterprises need to have a set of people who are located at the DR site to start the recovery and retrieval operations. Here the need for the right equipment is necessary and once an enterprise has these in place, it can take a breather that the data would be safe.

Many enterprises plan simulated attacks and bring their systems down to see if the BCP/DR is functional and the systems recover as planned. Few people within the organisation know about the plan. It also helps in understanding how others respond to such attacks and helps them prepare more effectively.

A senior IT official, on conditions of anonymity, cites the example of the DR initiatives carried out by the National Stock Exchange (NSE) of India. The NSE primary site is located in Mumbai with a DR site in Chennai. Data from the critical business applications are replicated at the DR site and can continue functioning from this site even if the site in Mumbai is not functioning.

Every quarter, the DR site takes over the central datacentre and the actual trading operations are performed from this site. The Recovery Time Objective or RTO is maintained during the process. In case of any disaster, the loss for the NSE on the daily turnover-based revenues in the wholesale debt market, capital market, and derivatives could be over Rs 8,000 crore.

To prevent such occurrences, many analysts and BCP/DR experts opine that the best plans for ensuring a basic BCP/DR can be achieved in three levels. At the first level, if something happens to the building in which the company operates from, it should be possible for employees to work from another office nearby which is connected to the first. In the second level, if employees are unable to access the business district where the building is located, they should be able to work from an office that is around 15 to 20 kilometres away. And at the third level, if the problem is citywide, the business should operate out of another city.

Invest, plan and test

Planning a BCP/DR process is one of the most essential steps to ensure that things fall in place and function exactly the way an enterprise wants it to. It begins with trying to foresee what challenges and obstacles could affect the enterprise systems in case of a disaster.

Take for example, a fire drill exercise conducted by a leading Mumbai-based IT company. It took them six months to plan the BCP/DR exercise, which involved 100 plus people that included the CIO and his team, various functional heads, the management and auditors. The company also appointed a BCP/DR coordinator to draft the objectives of the exercise, organised a steering committee that reviewed and approved those objectives, and then used a benchmark model to plan out the sequence of events and milestones that needed to be met along the way.

IT heads opine that enterprises need to invest in the BCP/DR process even during these tough economic times, so that they can withstand any natural or man-made disaster and recover fast to continue servicing clients, will be regarded high by the clients and more likely to get continued business. There have been reports that suggest many corporates are not going ahead with BCP/DR tests to save money, which in turn increases their business exposure to risk. Organisations with a strong BCP/DR plan can cope with major disruptions effectively, without significant loss to profitability, market share, customer attrition or brand impact.

"It is not possible for enterprises to financially justify the time and effort and the cost of developing, testing and refining a BCP/DR plan. Such a plan won't provide any immediate RoI. But not having one when disaster strikes can bankrupt even the strongest business," says Hemani.

This is also true for small businesses. According to Small Business Administration, a United States government agency that provides support to small businesses, small to medium-size businesses are most vulnerable in an emergency, making preparedness even more important. In a small business environment, an employee often plays multiple roles. Losing one employee could mean losing the capacity for several critical job functions. By planning ahead and cross-training employees, one could ensure that multiple people are prepared to handle critical business operations in the wake of a disaster.

BCP experts comment that the planning phase of BCP/DR starts with garnering management support and buy-in. Once this is done, other departments in the organisation should also be involved to build a BCP/DR team with someone at the helm who owns the BCP/DR piece. It could either be a business compliance officer or a risk head or in some cases it could be the CIO who is in charge of the BCP/DR process. The team then needs to identify risks and carry out a business impact analysis of critical applications. After the plan is completed, it should be made available to all the stakeholders in the company.

"For a BCP/DR plan to be successful there is a strong need to have a high level of user confidence and it must be planned meticulously .Though many enterprises have a BCP/DR strategy in place, there are only a few who have gone ahead and implemented the process in the way that it should be implemented," says Jayabalan Subramanian, CTO, NetMagic Solutions.

He adds that once an organisation has gone forward and drawn up the BCP/DR plan it is simply not a case of sitting back and waiting for the disaster to occur. It must be regularly tested and updated in order to prepare for the eventualities that lie waiting ahead. "By carrying out testing on a regular basis, the mean time to respond (MTTR) can be reduced. Many organisations have a prepared approach rather than a surprise element in conducting mock drills. This is because some of them are sceptical to see whether the BCP /DR plan will work well," he says.

The state of BCP/DR

The value of BCP/DR is gaining momentum and is being appreciated by corporate India much more than ever before. We conducted a survey of over 50 organisations across various verticals to gain insights on the issues and practices in this space. The need for BCM is self-evident once we look at the number of disruptions that the surveyed organisations have faced. More than half the respondents reported at least two significant business disruptions in the last two years.

The other key finding was that in majority of the responses, the primary driver for having a BCP/DR process in an organisation has been initiated by the IT team. It is time that business heads start making their contribution on this front.

In terms of BCP/DR spending, 32 percent of the enterprises stated that they will spend more than the previous year while 40 percent said that spends will remain unchanged.

We share with you the findings and views of enterprise CIOs in the following pages.