

Ministers of information

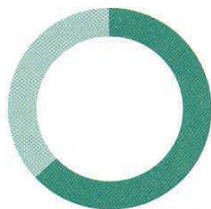
The recent terrorist attacks in New York have not only revealed massive national security breaches but also the dangers to business of information loss. **Parveen Bansal** reports

IN AN INFORMATION-LED economy, the failure of an information network is dangerously detrimental to business. Those without suitable back-up or recovery plans in place operate at their own peril. The September 11 attacks in the US not only raised a myriad of security concerns but also highlighted the importance of businesses having comprehensive disaster recovery plans to restore service as quickly as is possible – regardless of the severity of loss.

Business interruptions do not necessarily need to be on the level of a terrorist attack or an earthquake to affect significantly information availability. In fact, the most common threats are day-to-day logical disasters such as hardware corruption, database crashes or simple human error.

According to Hitachi Data Systems (HDS), “logical” disasters usually happen four times a year. The recovery time from these outages is 12 hours on average, or 48 hours a year. On a grander scale, natural disasters, such as fires or floods, occur less frequently, but are usually more devastating to the business as they result in loss of network hardware. Research by Gartner Dataquest on application downtime shows that an average of 40% of downtime is caused by application failures; 40% by operator error; and approximately 20% by systems or environmental failures.

1. Is reliability the most important factor when choosing an ASP?



■ Yes 63%
■ No 37%

Source: Seven Mountains

The consequences of computer-related downtime, coupled with an inadequate recovery solution, can be staggering. Although major operational risk losses are seen to have low probabilities, their impact can be large and perhaps exceed those of market or credit risks. An example is the effects of the system failure at the London Stock Exchange last year, which led to the dissemination of corrupted data, causing an eight-hour disruption to trading on the last day of the financial year.

Information is vital

Considering the high price of business downtime, organisations cannot afford any interruption that denies information availability. Because many enterprises that experience a disaster never recover, and an estimated two out of five enterprises that experience a disaster go out of business within five years (Gartner), it is no longer acceptable to recover data in three to four days. Recovery for the information economy needs to be immediate and automated.

Ludovic Leforestier, marketing manager, of HDS Europe, says: “The essence of disaster recovery is to preserve business continuity – to keep the most business-critical applications and systems running at all times to minimise downtime and avoid loss of revenue.”

He added, “It is not that companies do not have disaster recovery strategies in place already. A common problem is that companies make disaster recovery strategies and set up systems, but fail to conduct regular tests and find that not all of their data can be recovered. It is advisable to conduct tests quarterly and each time a new application is added to the current systems.”

Disaster recovery is essential but is often neglected by cutting corners. Mr Leforestier says: “Although the level of investment is very high for enterprise storage systems, they are, in fact, the most reliable systems – more than any other piece of software or hardware.”

Phil Jones, director of architecture and

technology at HDS, says: “Disaster recovery systems are like an insurance policy. You are always nervous without one and hope to never claim against them but, every so often, you have to.”

Location, location location

According to Gartner, in the early-1990s, business continuity was positioned mainly in terms of disaster recovery. In the event of a major disaster, technology assets were to be recovered in an alternate location. The typical recovery time objective (RTO) – the desired time to recover applications – was approximately three days. The typical recovery point objective (RPO) – the acceptable transaction loss – was 24 hours.

By the mid-1990s, business continuity initiatives had expanded to include recovery of critical-work processes, recognising the need for an alternate location as well as alternative human resources to man these centres, (eg, call centres). In the late-1990s, businesses began to understand the long-term implications of systems and application failure to their businesses. RTOs were reduced to less than 24 hours, and RPOs were often set up at the point of disaster – allowing no loss of work or transactions.

Take for example Dresdner Kleinwort Wasserstein (DKW), whose office was in the immediate vicinity of the World Trade Center and which was hit by power losses. Jim O'Connor at DKW says that by using remote shadowing software from Advanced Systems Concepts the company could restart business within an hour of the failure at their Manhattan site.

The problem was communicating and transporting the work of a staff of hundreds to the disaster recovery site. Its most critical system, the payment system, was running and able to continue with business as usual since information was replicated in real time to its disaster recovery site in nearby Queens.

It is recognising the widespread impact an outage can have on the financial markets