ENTERPRISE IT SYSTEMS do not, on the whole, work well under water, and their resilience is sorely tested when dunked in rank sludge. It's still too early to tell how much IT in the southern United States was ruined by the ravages of Hurricanes Katrina and Rita, but with just about every downtown office being computer equipped, the damage is considerable.

To the IT world, disaster recovery is underpinned by two principles. First, ensure that critical data, and even applications, are duplicated to a remote resource that is safely away from the danger zones – and any similar hazard. Second, plan for the strategic return to ‘business as usual’ after a disaster (be it fire or flood, earthquake or bomb) by having alternative IT facilities available – ideally by relocating existing staff to a new proxy IT centre.

Yet, according to market-watcher Gartner, about 40% of Fortune 1000 companies are not prepared for a regional disaster; small and medium-sized businesses are even less ready.

A poll conducted at Gartner's Data Centre Conference earlier this year on data replication architectures to meet disaster recovery (DR) strategies confirmed the analyst's suspicion that there's no single answer for all needs. There are, however, several effective DR strategies to choose from.

To work, DR needs to be well planned, well in advance. In general terms, organisations should first define their disaster recovery requirements in terms of cost, recovery time objectives, and recovery point objectives. Then they should design strategies, architectures and technology implementations (for example, specifying the type of replication) to meet those requirements.

Organisations shouldn't be concerned with finding a single 'right fit' strategy – this doesn't exist for all situations. Rather, they should implement strategies to meet their specific business requirements, Gartner counsels.

Assessors are still checking how well DR strategies in place in New Orleans held up to Katrina's onslaught. It will be weeks before the mud is hosed out of the corporate comms rooms around the city. As this happens, some very painful questions will arise.

The DR industry likes to think it can deal with most acts of fire and flood, but when both arrive together in the form of lightning strikes and burst levees, affecting such a huge metropolitan area, then even the best-laid DR plans are in trouble.

Disaster recovery has become a multi-billion dollar branch of the global computer industry, as companies and state departments have become mindful of the impact of hazards like flooding, lightning strikes, terrorism, and malicious criminal damage.

More savvy organisations are also aware that the siting of their core IT centres should be made with a view to potential threats. But this may not be an option for those tied to long-established quarters located in at-risk areas.

In New Orleans, any data centre sited below around six metres was submerged by the rising flood waters. This problem is exacerbated by the fact that many corporate premises have their IT rooms at ground- or lower-ground level – especially in older buildings.

This is partly because, in the past, it was associated with the facilities management departments that were traditionally sited on the ground or lower levels of single or multiple occupancy office buildings.

IT rooms have tended to remain low in buildings – a throwback to the days when computer equipment was so heavy that to place it upstairs would have entailed special – and expensive – strengthening of the architectural infrastructure. It was also thought to reduce the risk of water damage from above (faulty plumbing, roof leaks).

In the aftermath of the recent US hurricanes, as businesses move back into downtown New Orleans and the other affected areas, it seems likely that IT strategists will start to give more consideration to the siting of their systems than they did before.