Up in smoke

Recent months have proven just how fragile normality can be. From the tsunami that devastated Japan, to the huge protests of the Arab Spring, enterprises around the world have been reminded of just how important it is to plan for the worst. But just what is the current state of disaster recovery preparations in the region?

By Keri Allan

Never before have IT systems been so integral to the running of a modern business – be it large or small. But even though organisations are reliant on a wide number of applications and resources to access, store and process business critical information, it seems not all consider business continuity planning a high priority.

"A recent industry survey with the Business Continuity Management Institute revealed that almost 70 per cent of the region's organisations have not put in place a robust disaster recovery or business continuity management programme, despite major disruptions and disasters caused to businesses in the region," notes Steven Huang, head of Enterprise Solutions and Marketing at Huawei Middle East.

However this mindset looks like it may be changing as companies begin to grasp that disasters on the other side of the world could possibly affect them. "With global IT infrastructures we don't just contain issues to our own region, but can be effected by disasters around the world," notes Paul Sherry, regional sales director, Riverbed Technology. "Interdependencies between databases can span countries, even continents. These are all considerations when building disaster recovery and business continuity plans," he adds.

Even so, the smallest problem locally can also affect a business' productivity, so disasters both home and away must be prepared for.

"Disasters in the Gulf region may not be as dramatic as an earthquake or flood; but power outages and surges, damage to undersea telecommunications cables, malicious code attacks on computer networks and structural failure in buildings are all instances of disasters that can cause a great deal of damage to a business," says Anthony Harrison, solution architect, Symantec. "But it must be noted that software and hardware failures count for a large proportion of disasters. It is important that a business consider these 'everyday' occurrences as potentially disastrous for their business – a disaster that can halt or impede their

IN NUMBERS

70%

The percentage of Middle East enterprises that do not have a disaster recovery plan in place.

21%

The percentage of executives concerned about the risk posed by natural disasters.

Source: BCM Institute report

ability to service customers and generate revenue," he adds.

Another consideration that has brought the importance of business continuity to the forefront has been the Middle East's current political situation. Many companies are giving more credence to these plans as the unrest means that there is a greater risk of power cuts or even building damage.

"These companies have often deployed solutions quicker than most implementations, because they are keen to protect their IT systems in the event of an unexpected disaster," explains Wouter Vancoppenolle, director of sales Middle East and Africa, Vision Solutions.

But with the region in general still in recovery mode from the global economic downturn, how willing are businesses to spend funds on such areas? It appears that the countries affected by political unrest are putting business continuity higher on their agendas, but overall companies are finding that disaster recovery is important enough to spend money on.

They may not be buying the most 'hefty' of solutions, but are looking for fairly priced, robust offerings. Many are playing a balancing game between what they'd like to have and what they can afford, but are compromising in a way that still keeps them covered.

Because IT is what keeps a business running it's clear that CIOs play a crucial role in any business continuity plan. Their role usually entails managing the overall IT operations for a company so when something goes wrong they will be the ones the business turns to for answers. However they should not work alone, but include their board level counterparts.

"My view is that the CIO needs to be raising the subject of business continuity and disaster recovery planning with his counterparts so that the subject has executive board level visibility," highlights Steve Langley, technology consulting, EMEA, HP.

"The CIO should be a stakeholder in the plan but not necessarily own it as this needs to reside with the COO or indeed CEO. The CIO needs to provide IT solutions to support the plan but not decide on behalf of the business the requirements and the trade-off between risk and cost," he notes.

Part of disaster recovery planning is to work out the most mission critical systems the business uses and then to set a recovery point objective (RPO) and a recovery time objective (RTO) in order to be aware of what needs to be done and how quickly.

"The RTO is how long the company can be 'down' for; that is. how long it can go without normal operations before it causes too much damage to the business. The RPO is the point in time that the business needs to recover to. For example, an SME may be able to handle losing two to three days worth of data, but a large financial organisation may not be afford to lose more than an hour's data," explains Vancoppenolle.

Of course risk profiles will vary dramatically from company to company, even city to city, so Langley recommends that each company undertakes a full risk analysis during the planning stage.

"The generic risks of loss of power, flood, terrorism, seismic disturbance and pandemics all need to be looked as well as any specific industry related risks (i.e. drug testing company attracting the attention of animal rights campaigners, or a board decision resulting in the attention of hacktivists, such as Paypal, Mastercard or Sony Computer Entertainment)," he notes. "The organisation should then prepare mitigation and crisis plans for each scenario based upon a likelihood/impact analysis."

Data loss can be the death of a company if it is unprepared for the possibility of it.

TOP FIVE CONSIDERATIONS

Deciding what are the most important things to cover with any disaster recovery plan, it can be a daunting process. There are any number of possible disasters, and while some are more likely than others, many require different approaches to ensure that your company's risk exposure remains low. However, there are ways to ensure that you manage to achieve that, without necessarily looking at individual solutions, or disasters themselves.

According to storage experts Nasuni, the top five factors that should be considered when looking at any disaster recovery and business continuity solution are the minimum amount of downtime any solution will require, the integrity of the data in terms of each storage methods, the cost, its simplicity, and the security of it – both in terms of protection from disaster, as well as theft.

When it comes to the kinds of solutions out there, there are many different levels depending on the depth of 'back-up' solution a business wants.

Sachin Bhardwaj, head of Marketing and Business Development, eHosting DataFort breaks down the solutions into three

"Organisations should prepare mitigation and crisis plans for each plausable scenario based upon a likelihood/impact analysis."

"Placing disaster recovery outside of an firm's own facilities may provoke data concerns, but if disaster strikes city-wide, it can wipe out the back up too.

scenarios, which are classified as hot, warm and cold sites.

"A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real time synchronisation between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialised software."

The 'always on' technology concept would be a hot site solution for example, which allows a company to never stop running no matter what it faces.

"The 'always on' solution is based on adding an extra network tier that can facilitate the recovery by intelligently forwarding the user requests toward the resources at the best available location," explains Tarek Abbas, Systems Engineering director, MENA, Juniper Networks. "This applies to both local and remote users. This tier is called the secure access web tier."

A very expensive solution requiring a heavy technology and manpower investment means that, to date, take up of 'always on' solutions hasn't been high. However, certain industries feel that the cost is worth it. These are sectors such as aviation and defence as certain technologies are critical to their business.

"A cold site is the most inexpensive type of back-up site for an organisation to operate," says Bhardwaj, moving on. "It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

"A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have back-ups on hand, but they may not be complete and may be between several days and a week old. An example would be back-up tapes sent to the warm site by courier."

Certain solutions can provide further issues too. For example, as more and more companies look to push their secondary datacentres further apart they need to ensure the communications between them have efficiently performing WAN links, such that in the event of any disaster they RPO and RTO can be met. WAN optimisation solutions are appearing in response to this need, from companies such as Riverbed Technology.

So what is the most popular solution chosen currently?

IN NUMBERS

93%

The percentage of companies who went bankrupt within a year of having an outage of 10 days or more.

Source: Global Data Vaulting

IN NUMBERS

44%

The percentage of virtualised data that isn't backed up regularly at enterprises globally.

70%

Of enterprises have experienced outages due to power loss and other power failures.

Source: Symantec Disaster Recovery Report

"Most companies only really invest in hardware 'mirroring' and off site back-up solutions. This appears to be the most popular form of disaster planning as it covers the 'disasters' most often experienced as well as being reasonably cost effective," says Huang. "Battery back-up with diesel generator failover in the event of complete power failure is also employed, but not as widely as perhaps it should be in this region. Co-location is not widely used and would only really be effective as a disaster recovery solution if the co-location site were to mirror the organisation's own IT infrastructure.

"Placing disaster recovery solutions outside of an organisation's own facilities will provoke concerns about customer data security. Therefore, co-location and public cloud based solutions might not be acceptable solutions. For this reason, it would appear that a full and effective disaster recovery solution involving separate customer owned facilities is the solution that is often most considered," he concludes. ACN

Keeping other board members up to date with disaster recovery plans is crucial.

NOT JUST POLICIES

With any disaster recovery solution, it is important to regularly review it and ensure that it is still suitable for the present situation. One example of a company doing just this is Qatargas. Years of rapid expansion had seen it outgrow its existing IT infrastructure. It had also begun relying on a second disaster recovery website. One small piece of the infrastructure that was having a profound impact was its wide area networking facilities. According to Qatargas, employees in the company's branch offices were finding it difficult to access files stored centrally over the network, while the slow network was also impacting its ability to back-up data from remote locations. Upon upgrading, it saw a 70% improvement in data back-up speeds, proving that not all disaster recovery considerations are policy based.