Disaster recovery 36
February 2011 Vol.17 No.02

Act before it's too late

It doesn't take a natural disaster to bring down IT operations. Companies need a disaster recovery strategy that allows them to continue working when things go wrong.

A sudden event can bring down the most robust IT system at any moment. On the rare occasions when it does happen, organisations are often unable to recover key data and resume operations.

The term 'disaster recovery' tends to bring up images of bad weather, flash floods or fires. But in a region like the Middle East, with its relatively benign weather, hacking, data loss or system failure are probably more likely causes of the kind of disaster that can take out a corporate IT system.

According to Symantec's '2011 SMB Disaster Preparedness Survey', which focused on small and medium sized businesses (SMBs), attitudes towards IT disasters remain almost entirely reactive.

This, despite the fact that a disaster can render a company unable to operate and jeopardise long term operations. Downtime not only costs money, it also causes annoyed customers to leave when services are unavailable.

"According to the research findings, SMBs still haven't recognised the tremendous impact a disaster can have on their businesses. Despite warnings, it seems like many still think it can't happen to them," says Saurabh Arora, manager, small and medium business for MENA, Symantec.

The company's survey included 1288 small and medium businesses with five to 1000 employees and 552 customers. All regions of the world were surveyed.

Half of the respondents do not have a disaster recovery plan in place. Forty one percent said that it never occurred to them to put together a plan and 40% stated that disaster preparedness is not a priority for them. Only half of companies surveyed back up at least 60% of their data, and less than half back up their data weekly or more frequently. Only 23% back up daily.

Key data is not always backed up, either. Of those surveyed, 31% do not back up email, 21% do not back up application data and 17% do not back up customer data.

Respondents also reported that a disaster would cause information loss. Forty-four percent of SMBs said they would lose at least 40 percent of their data in the event of a disaster.

"Disasters happen and SMBs cannot afford to risk losing their information or, more importantly, their customers' critical information," says Arora. "Simple planning can enable SMBs to protect their information in the event of a disaster, which in turn will help them build trust with their customers."

Tareque Choudhury, head of security practice and professional services, MEA, BT Global Services, adds: "Organisations within the GCC tend to underestimate the likelihood of disaster striking them. It is difficult to determine how likely it is that an organisation will face disaster, but every company should have a disaster recovery plan at a minimum with thoughts on having a complete business continuity strategy."

According to Mohamed Rizvi, manager of Information Security and Advisory Services at eHosting DataFort (eHDF), there are different types of incidents

Disasters happen and SMBs cannot afford to risk losing their information or, more importantly, their customers' critical information

that may qualify as disasters and that may strike at different levels of magnitude.

"These could be site outages due to earthquakes, floods or fires; logical outages due to virus attack, memory leak or data corruption; and partial outages due to hardware failures or software failures," he says.

Stability of IT systems has increased dramatically over recent years, along with increased awareness, yet weak points do still exist in hardware, mainly due to mishandling and component failures.

"In this kind of a scenario, better performance is achieved by providing a proper data centre environment that includes high end power and cooling systems and state-of-the-art infrastructure that is capable of withstanding disasters," says Rizvi.

A disaster recovery strategy should encompass five key steps: processes, policies, procedures, technical arrangements and vendor arrangements.

Any organisation that hasn't done so should act now by identifying the resources that need most protection. These are the IT assets, most likely customer data and financial information, without which the company would not be able to function.

Having identified them, the risk of loss needs to be reduced by applying anti-virus updates regularly, password protecting the data and eliminating the possibility of accidental overwrites. End users also need to be educated in the basics of good computing practice.

From there, organisations can began to look at more cash and technology intensive measures such as automated backup.

In an ideal scenario, offsite backup will form part of a disaster recovery solution. Bandwidth, and thus the cost of offsite data backup, is costlier in the Gulf than in most other regions, but Rizvi at eHosting DataFort believes organisations must consider it seriously.

"To make offsite backup affordable or viable, the cost proposition of such a solution has to be looked at in different ways," he says.

"Disaster recovery strategies can be based on a cost benefit analysis at the planning level. There exist disaster recovery solutions where optimum use of small bandwidth is possible by controlling the utilisation of bigger bandwidth.

"This will help the organisation to maximise its return on investment from a DR solution. Even among our customers, we have provided customised solutions to control bandwidth costs," he explains.

The amount of bandwidth that would be needed to manage offsite data backup is hard to quantify, and the storage itself can be costly. This is where organisations would have to make a cost/benefit decision on which data absolutely must be backed up, how often and how to free up bandwidth.

"Organisations should carry out a proper due diligence of their business and determine the value of their data and which portions of it should have a backup kept offsite," says Choudhury at BT. "Determining bandwidth requirements has so many dependencies such as types of applications, applications usage, amount of users and frequency of backups."

Cost notwithstanding, offsite backup has been seen as a hard sell in the region. It isn't an ever constant necessity and ends up being seen as a luxury, despite the fact that it could one day be the thing that saves a company.

"Offsite backup is taken up by organisations depending on the criticality of the service and the threats the service is exposed to," explains Rizvi at eHDF. "Today, CIOs and IT managers are looking at DR solutions very closely and most organisations need a secondary site as a


Saurabh says many companies think 'it' won't happen to them.

Disaster recovery strategies: Key steps

- **Act now.** Don't be trying to retrieve a situation after a disaster has happened. Immediately identify the resources that need most protection and build on the plan from there.

- **Reduce the risk of loss.** Ensure anti-virus subscriptions are up to date and data critical to the running of the business, such as customer records, is adequately protected. This reduces the risk of cyber theft and accidental deletion.

- **Backup.** Have key data, such as customer records and financial information, backed up regularly – not only to an internal backup drive, but also to an external location. Bandwidth may make external backup costly, so organisations need to ascertain what is most critical and prioritise. Many organisations could free up more bandwidth than they realise by having stricter internet usage policies.

- **Educate.** Not all employees are power users, but they should know the basics of computer security and what to do if information is deleted or cannot be located.

- **Test.** Updates may not be administered automatically and data backups may not occur when they're supposed to. Remember to regularly check that these things are happening as they should.

- **Review.** Regularly revisit disaster recovery plans, especially in the light of hardware or software changes.


Rizvi: The value of offsite backup comes down to cost versus benefit.

backup site to run their business along with having a primary production site.

"They understand the business challenges and realize that making IT services available to business is their priority. Therefore, based on these priorities, DR solutions are chosen and are not considered as luxury. It has become an important component of IT and business as the threats landscape has increased substantially in today's environment."

Choudhury at BT identifies offsite backup as an area where the end user in the region still needs some convincing. "The regional market still requires a lot of education on backup strategies and overall business continuity," he says. "The larger enterprises seem to be doing well when it comes to disaster recovery, but the SME market has some catching up to do."

In addition to offsite backup, some backup providers can also offer disaster recovery 'seats'. This enables companies to rent physical space in premises run by their disaster recovery provider. In the event of disaster, this allows key employees to quickly be at a desk, with full access to a phone, PC and their company's backed up data.

The typical cost of downtime for an SMB in the Symantec survey is US $12,500 per day. Ultimately, it makes good business sense to have a disaster recovery strategy of some kind in place.