GANG-NAIL GUIDELINES No.107

ANOTHER MITEK ADVANTAGE

IT DISASTER RECOVERY

By JOHN GARDENIERS
Information Systems Administrator
MiTek Australia Limited

Most medium and large organisations have a Business Continuity or Disaster Recovery plan. Such plans are seldom formulated or implemented for smaller organisations, although the reasons for having them are the same.

Disaster Recovery, as it applies to IT, is the ability to bring computers and network systems back to pre-disaster operational mode in the shortest possible time.

A disaster can include the complete loss of data, programs and operating systems up to and including the loss of hardware such as might happen in the case of a building fire.

There are of course two aspects to Disaster Recovery.

1. The information required to reinstate a system must previously have been saved, together with the data that is to be restored.

2. A means must exist for the system to be recreated and the data restored, allowing business to continue.

SAVING INFORMATION AND DATA

The first step is to determine just what needs to be saved or backed up and what doesn't.

While it is obvious that all business related data, such as the data for those orders you are processing, should be backed up, it may not be immediately obvious what other information is vital.

Here are just a few areas to consider.

- Security related information, such as passwords, together with details of where they are used and what restrictions may apply.
- Business contact details; valuable information that can take a long time to replicate.
- Any special information required for setting up connections between components, such as PC's and factory machinery.

Once you have gathered and saved the information you deem critical and made up to date data backups, what are you going to do with this information?

Ideally it should be taken off-site each day. Where and how it is stored is something much discussed in IT circles. Generally there is a trade-off between what we would like to do (stored in a fire-proof vault at a remote location, secured by armed guards and vicious dogs) and what is feasible and affordable.

The most common approach is to take it home at the end of the day. If you do, just be aware of any consequences of losing this information or having it stolen. If you feel more comfortable storing recovery information on-site then it really has to be in a suitably rated fire-proof safe.

RESTORING IT

Should the worst case occur and you need to reinstate your systems, the information and data you have saved should allow you to do so with reasonable ease.

Obtain the computers you require, reinstall the software, restore the data and configure any special details, as per the previously saved information. If all has been done correctly you should be able to have at least a basic IT infrastructure operational again very quickly.

If the above sounds overly simple it's only because a well formulated and implemented Disaster Recovery Plan does indeed make recovery a relatively simple process.

TEST IT!

Don't wait for a disaster before finding any flaws in your system. Test your plan from time to time or whenever any significant changes are made to the IT infrastructure. When weaknesses are discovered, correct them.

Testing involves being able to restore your systems and data, while simulating a disaster. For example using a spare computer to restore to as your file server, using the information and data you have backed up.

Ensure other vital information, such as passwords, can in fact be restored from whatever media you have it saved to (which might be something as simple as a paper notebook).

If it doesn't work during your test it's not going to work when the very survival of your business may depend on it.