GANG-NAIL GUIDELINES No.152

ANOTHER MITEK ADVANTAGE

PROTECTING YOUR IT ASSETS

Almost all truss plants, and in fact almost all businesses, are reliant on computers.

Despite this, it is still surprising how many businesses have no comprehensive protection against that unforeseen mishap.

Although computers have many benefits, they are prone to some unique dangers (apart from the normal risks of fire and burglary) - virus attacks, hard disk crashes, hardware (eg. CPU, RAM) failures, etc.

To keep a plant running smoothly a Business Continuity Plan (BCP) is a good approach.

A BCP will include an IT protection plan - a plan for the general protection of your IT assets, including Disaster Recovery.

IT PROTECTION PLAN

A starting point would be a risk assessment of your IT assets.

Define the importance of various pieces of equipment, the risk of something happening, supplier availability and how long you are prepared to wait to rectify a problem in the event of an unforeseen event.

How long can the business manage without computer access?

For example, take a plant with say three detailers. One could say that the odds are against all three pc's being out of action at the same time, so management may be prepared to accept that risk.

However if one pc fails, consider how long management would be prepared to wait for the designer to be productive?

If there are no spare pc's available, he/she could be unproductive for several days, so it may be wise to have a spare unit available or know where to find a replacement quickly.

Consider also the need to access a backup of your data.

Back-ups are the king pin of any IT protection plan, whether it is to recover a machine after a virus attack, to restore accidently deleted data, or loss in the event of a disaster.

By MARTIN SHICKLE
IT & Computer Services Manager, MiTek Australia Limited

Points to consider:

- Create a backup process which is well documented and assign responsibility.
- Decide what data needs to be backed up. Email, job data, accounts, your holiday pictures?
- Decide on frequency of back up. If things go wrong, what is the longest period you are prepared to lose data for?

Remember your data is only as good as your last backup.

DISASTER RECOVERY

Disaster Recovery is focused on preparing for the recovery or continuation of technology infrastructure, which is critical to a business.

The key question, if disaster strikes, is how quickly do you need each part of your operation to be back up and running?

This may be a balance between speed of recovery and cost.

For example some businesses pay for office units with pc's etc. available and 100 per cent failover, so if a disaster strikes, staff transfer to the office units and carry on working.

Not a cheap option, but for some businesses, super critical for ongoing service.

VIRUS PROTECTION

Good antivirus software is essential.

A 2009 security survey found that 33 per cent of Australian small businesses lacked basic antivirus protection and that malicious spam and phishing attacks were on the increase.

If cost is a factor there are free versions of antivirus software available, but keep in mind, cost versus loss of data, may be a misleading guide.

Make sure:

- all computers have virus protection software installed and running;
- the virus protection data is up to date;
- all pc's have the latest operating system updates installed (these often include fixes for security vulnerabilities);
- ensure appropriate firewalls are active; and
- a security awareness program is implemented, along with training and guidelines, so everyone understands the security implications of online behavior.

ELECTRICAL EQUIPMENT PROTECTION

Power problems such as surges, spikes and blackouts can cause a loss of data and damage to electrical equipment.

Protection can come in a number of different forms such as:

- Power boards with built-in surge protection. These devices are generally designed to fail after one surge - check and replace when needed
- Uninterruptable Power Supply (UPS). A UPS will provide emergency power when the mains power fails. Some are also designed to protect electrical equipment from electrical problems such as surges, spikes, noise etc.

Don't forget that you need to prove any processes you put in place, like having a fire drill; you should simulate issues and check that procedures work.

This is just an overview of what needs to be considered in the formulation of a BCP. If your operation is too small to have permanent IT staff, seek advice from an IT support professional. TTN