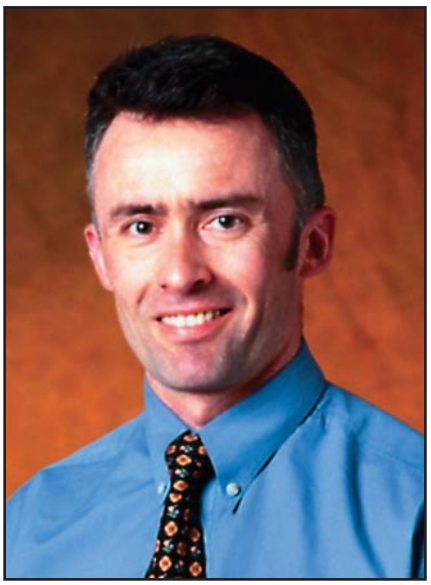
I.T. NEEDS YOUR SUPPORT



By ANDREW SCANE

IT & Computer Services Manager

MiTek Australia Limited

Some of the calls that make IT support staff nervous start like "I think I've just deleted…"; "I think I have a virus"; "We've been broken into"; "There was a storm".

Instead of a confident response along the lines of - "No problem, just restore from your back ups."

"The virus should be detected and removed automatically."

"Your computers and network will be protected by . . ."

The first question is usually – "Please tell me you have a current backup."

Do you have any anti-virus software installed? Is it up to date?

Do you have any spike/surge protection on your network?

Sadly, there are still more no's than yes's to these questions.

There's no fun in telling an often-desperate caller that all the data is lost and he or she will need to start over.

In a previous GN guideline (No.28), John Tadich discussed the subject of data security and outlined many of the issues affecting truss plants.

It is encouraging to see over the last few years how some fabricators are now taking IT management seriously and have given it the respect and investment that it deserves.

Although the size of the business will usually dictate the amount of investment, like it or not, computers and electronic communication are part of our everyday lives and we cannot afford to ignore the consequences of data loss.

Consider the implications of losing all your computers and data due to theft, fire or a disaster such as the corruption of you data from a virus attack or loss of data due to a power surge or sag.

Do not underestimate the value of your data. How much time will it take to rebuild the data and how much business will be lost in the meantime?

Let's take these few issues and see how prepared you are and how well you can recover.

In the following table place a tick in the Yes or No column to indicate your current situation.

The exercise could be well worth the effort!

	Yes	No
Back-ups Do you back up your computers (data, jobs etc.)?	👍	👎
Daily Back-ups?	👍	
Weekly backups?	👍	
Do you keep permanent copies of the weekly / daily data?	👍	👎
Are backups kept off-site	👍	👎
Do you check the integrity of your backups	👍	
Disaster Recovery Do you have a disaster recovery plan	👍	
Have you performed a recovery using your disaster recovery plan	👍	
Virus protection Do you use virus protection software	👍	👎
Is it kept up to date?	👍	👎
Surge protection Do you have lightning protection on network ?	👍	👎
Is your power supply protected for surges and sags?	👍	👎

Now count up your 👍 and 👎's.

The more 👍, the better your situation.

Unfortunately any 👎, means you have a risk that needs to be addressed.

Here are a few tips that may help in addressing any 👎.

Back-ups

- Make someone responsible for your backup system and ensure the backup system is documented, understood and can be carried out by more than one person.
- An important part of the design of a back-up system is to establish what you can afford to lose, what needs to be kept permanently and what is kept off site.
- The back-ups need to be regular, systematic and on going.

Disaster Recovery

- The cost to a business during the down-time required to restore computer systems and data will often help to determine the most suitable disaster recovery solution.

Anti-virus

- The selection of an anti-virus package should be made to ensure it is providing adequate protection. Don't just pick the cheapest package available at your local shop.
- It must be kept completely up to date at all times. This can be achieved by downloading updates and upgrades via the Internet. This critical point is often overlooked or ignored. Weekly updates should be the minimum.
- It must be running. There's no point in having it if it's not being used.
- When enabling sharing on computers over networks, do not share the root of drive C: or the Windows folder as these are easy targets for some viruses.
- To avoid virus infection of networks, computers with internet connections via modem should not be connected to the network, unless it is through a firewall.

Surge Protection

- Power problems, usually surges, spikes or blackouts are the largest single cause of data loss.
- Many lower priced surge protectors are good for only one surge, so this should be considered before making a purchase.

Responsible management of your IT investment includes the identification, assessment and addressing of risks. Planing for risk is essential in today's business.

Understanding the full extent of the consequences will help in the planning of the solution.

Do not delay in addressing any risks that you may have identified in your business as there is plenty of help available for responsible IT management.

Get advice from an IT support professional.

These are the calls they look forward to!