Gang-Nail Guide Lines No.28

DATA SECURITY - WHAT NEEDS TO BE DONE?

by JOHN TADICH
Technical Services Manager,
Gang-Nail Australia Limited

Truss plants are becoming increasingly reliant on computers. A few years back we only saw the odd computer in the Estimating and Detailing office, but today there are not many plants that don't have one or two on the factory floor as well.

Have you considered how your business would cope if you lost the use of all your computers overnight? Most plants would, I think, be out of action for quite some time.

This would most likely result in a large number of upset customers, possibly lost forever, and a large reduction in cash flow, not to mention the loss of profit. An event like this could cause a business to fail.

Although computers and application software could be replaced in a few days, your quotes, detailed jobs and business data may be lost forever if proper backup procedures have not been observed.

You may think that this is an unlikely occurrence, but when you consider that only one of the following events could cause the loss of your *business' life blood data.*

1. Computer viruses.
2. Technical malfunction of storage media.
3. Human error.
4. Theft/Sabotage.
5. Lightening.

These are just a few events that are more important with regard to computer data. Events like flood, fire and storm damage will obviously cause similar loss of data along with more wide spread havoc. However, I would like to concentrate on these higher risk and more controllable events.

In IT circles they talk about two types of data:

* Data that has been backed up
* Data that has not been lost - YET!

I do not think I need to convince anybody it is so essential that all computer software and data be backed up. But, how many of us do this satisfactorily?

BACK UP RECOMMENDATION:

- On a daily basis, backup all data on to a reliable media.
- Regularly restore data to test the systems integrity and media reliability.
- Back ups should be rotated off site in case of fire or theft.
- On a weekly basis backup all data with application and system files.

However, to restore your data can take a considerable amount of time and you inevitably loose some of the most current data. So backups are really our last line of defence and should not be our **only** line of defence.

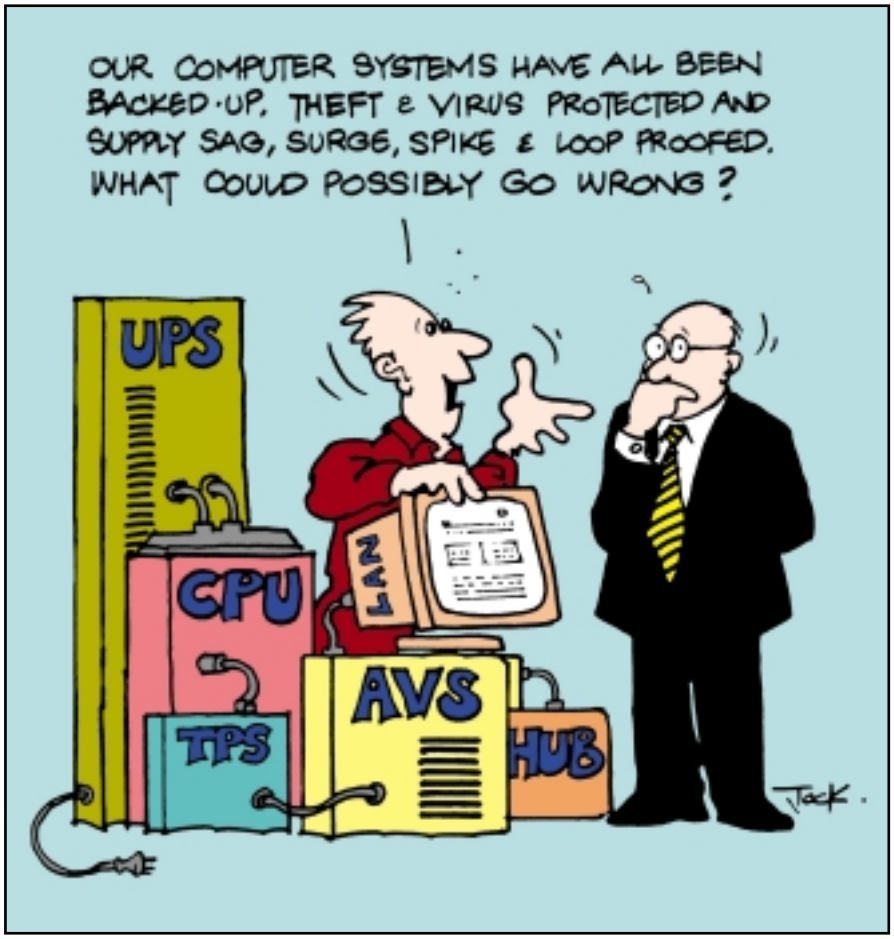
What else can we do?

Virus Detection

As computer viruses are becoming more common, virus detecting software should be included as an essential piece of software for any office. However, it is not a matter of buy and forget.

As there are new viruses by the day, you must select a supplier who has the resources to keep up with the new

Continued on next page



Gang-Nail Guide Lines Cont.

viruses and be prepared to purchase and install updates, as they become available.

Hardware and Equipment

Damage to hardware and subsequent loss of data is frequently caused by power disturbances. These can take the form of:

- Spikes - usually lightening induced.
- Electrical noise - induced by electric motors.
- Sags - drop in voltage.
- Surges - increase in voltage.
- Blackout - complete loss of power.

Damage due to power disturbances may not be immediate but it can have a cumulative effect causing degradation over long periods of time, eventually causing the system to crash for no apparent reason.

The solution to these power problems is to condition the power using an Uninterruptable Power Supply (UPS). These devices are relatively inexpensive costing $200 to $300 per workstation.

As well as filtering out spikes, sags, surges, etc the UPS provides battery backup power in the case of blackouts. As the majority of blackouts are of less than 10 second duration, the UPS allows the users to keep working without loss of current data. In the case of longer outages it allows the computer to be shut down normally, reducing the risk of damage to the hardware or loss of data. Intelligent uninterruptable power supplies are also available, which will shut down the computer in an orderly manner should the operator not be in attendance at the time of the blackout.

Local Area Networks (LAN)

Network servers should also be protected by a UPS. In the case of servers it is essential that they have sufficient backup power to do a complete shutdown and have the ability to carry out the shutdown process automatically.

LANs should also be designed using star topology (e.g. hubs) to avoid problems with individual faults bringing down the whole network, as could be the case with bus topology network systems, e.g. Daisy Chain.

Where LANs include factory areas or where they link remote workstations (greater than 185m), Fibre Optical cables should be considered. Fibre Optical cables will eliminate lightening induced spikes through the network as distinct from a spike in the power supply. The cost of Fibre Optics has reduced significantly and should be your first choice for networks which cover large areas.

Automated Machinery

With the increased dependence on computer controlled machinery in truss plants, we must also take similar precautions to ensure continuity of service. These automated machines tend to become pivotal to production. In most plants, if they fail, production would grind to a halt. There are a number of things we can do to minimise problems with this type of equipment.

1. **Computer Protection at Machine**

   Truss plants, by their nature, are very noisy electrically, with saw motors, compressors etc. starting and stopping. Therefore, a line filter is highly recommended. A DIN Rail type filter mounted in the machine's electrical cabinet provides adequate protection. A Total Power System (TPS) Model DIN-16 available from most electrical wholesalers would be suitable.

2. **I/O Card Protection**

   Earth loops between computer and PLC can develop on some machines, which cause problems with I/O cards. This can be resolved using an optical isolator in the RS232 line between saw computer and PLC. P/N648-942 from Farnell Components would be appropriate for this application.

3. **Networks**

   Whenever computer controlled machines download data through LANs the network *Hub* should also be protected using CAT5 Network Transient Protection.

These recommendations may seem daunting to those not familiar with electrics or electronics, however, do not dismiss the security of your data and electronic systems because it all seems too difficult.

The principles are well understood by most competent electricians and network specialists. All you need to know is that there is a potential risk in each of these areas, and that the ongoing success of your business may depend on you taking action now.