Things that you should know about your IT systems

In this hectic World it is too easy to believe that your IT systems are working without fault. Most businesses never give them a second thought until some emergency develops. In many cases, it becomes impossible to successfully recover from an emergency because something critical hasn't been working for a while and nobody knew.

The aim of this document is educate business owners on what we consider the critical things they should know about their IT systems. Someone should be able to perform all items on this checklist ***WITHOUT*** assistance from your IT support organisation. Because, happens if you can't get in contact with them and you need an answer immediately ? If you are able to perform all the items on the list below then, in a crisis, you stand a much better chance.

1. How to reboot a server or workstation

The first step in resolving many issues is normally to reboot the system. The impact of rebooting a workstation is usually only a minor inconvenience to that user. On the other hand rebooting a network server will usually inconvenience every user connected to the system. In some cases, to reboot a server, you may need a different login and password to commence the reboot process. Ensure that a suitable login and password are available and you are familiar with the process.

Sometimes when you attempt to reboot a server or workstation it may get "hung" up for some reason. If so, then the only resolution maybe to reset or power off the machine. In this case you need to know where the power button for the machine is and how to use it (in most cases holding the power on for a few seconds will switch the machine off). Secondly, you should also know if there is a machine "reset" button (not all machines will have one of these). A 'reset" button can be used to restart your machine in case of a system hang. If all other reset options fail then you need to know how to power off the machine via the power point or by pulling the plug physically out of the machine.

2. How to check backups

The major insurance policy that any business has for their information is backups. Because most cases backups are scheduled to run automatically overnight most businesses are under the mistaken assumption that they always work. This has been proven tragically incorrect for some businesses who didn't take the time to check regularly. One such business mistakenly write-protected all of their tapes, while another had a tape drive malfunction. In both cases no data was ever written to tape and it was only discovered when they desperately needed to restore.

Do not underestimate the value of your data. It is what keeps your business operating, you should therefore treat it like gold. You should be checking your backup logs every day to ensure correct operation. Backups can fail occasionally for different reasons but constant failure is a matter that needs to be urgently addressed.

3. How to restore a file

If you are successfully backing up then that is only half the battle. At a very minimum you should know how to at least restore a file from your backups. The information stored on your file server belongs to you and therefore you should be in control of it. Not being able to restore a file will mean that, in an emergency, you may have to wait to contact someone who knows how to do the restore. What happens if that person isn't available for a long period of time, say over a weekend ? Could you afford that ?

You shouldn't just restore something once and then forget about it, you should restore some data from your backup on a regular basis. Firstly, this will give you practice in the restoration process and secondly it will ensure that the information on your backup can actually be restored. Even though a backup reports as being good, you are never completely sure until you actually do a restore. You don't want to find out that your backup is empty at the most critical time !

4. How to disable a user

Every user on your network should have a unique set of rights that gives them access to information on your server. You potentially need to be able to prevent a user gaining access to this information for the some of the following reasons. Firstly, what happens when you terminate an employee ? You don't want them being able to access their information either on a desktop or remotely. If you suspect that a user's account has been compromised in some way you need to be able to disable it to reduce the threat of compromise.

5. How to change a password

You need to know how to change a password. Firstly you need to know how to change your own password and secondly you need to be able to change the password of any user on your network. Typically you will need to do this when a user forgets their password or it expires and they can't login to the system. Passwords on non Windows 98 systems should always be greater than 14 characters and should be a pass phrase rather than a password. For example it is much easier to remember something like "my dog and I went to the zoo" than "v27bw992n-02o2lk2-0".

Remember, passwords are the last line of defence between you and someone who wants to gain access to your system. The stronger the password the more unlikely it will be to be compromised. Remember, your system is only as secure as your weakest password.

6. How to check date of virus signature

Antivirus programs are a reactive technology, they work by scanning incoming files for a certain signature of characters. You need to know how to check that you do have current signatures for your antivirus program. Again, this is not something that you

can check once and then forget, you need to perform this on a regular basis because it is possible for the signatures to stop downloading.

7. How to scan for a virus

No matter how up to date your virus signatures are it is still possible for something to slip through. Therefore you should know how to run a virus scan on your machine to ensure that it is free from viruses.

8. How to check your system is up to date.

Most viruses and external threats to your system normally exploit some vulnerability with software that resides on your machine. Once again the process of keeping your software up to date is on going. When any software program is released it is normally as stable and secure as it can be made, however as time progresses vulnerabilities may be found in situations that the developers never thought of. In this case they will release patches to fix these vulnerabilities.

To keep your system up to date you need to install these patches on your system. With so many software programs installed on machines it is very hard to keep them all up to date. At a very minimum you need to keep both your version of Windows and Office up to date. Patching these products will go a long way to preventing attacks.

9. How to recover from a disaster

As they say "if you fail to plan then you are planning to fail". Too often a disaster recovery plan is over looked by a business. Not only should you have a disaster recovery plan for your IT systems, you should have one for your whole business. A disaster recovery plan will help you plan for and answer questions such as : How long will it take me to get working again ? What happens if this component of my business fails unexpectedly ? Whom do I call when I am faced with these sort of disasters ?

We all hope that we never have to use our disaster recovery plan but it is clear that businesses with a well planned and documented plan stand a much better change of continuing business in the face of unforseen tragedy.

Conclusion

It is our firm belief that every business that depends on IT systems ***MUST*** have confidence to perform each and every item on the above list without external assistance. If you don't, then you are putting the fate of your business in the hands of someone else and that is a major risk.

The simply solution if you haven't already is ***DOCUMENT.*** Do it now before it is too late !