

Disaster Recovery – Business Continuity

- If your servers/computers failed, would your business be able to keep trading?
- If a business near to yours is the direct victim of fire or flood and emergency services prevent access to your premises for days, could you still operate?
- If your network was infected by a virus, could you switch to other virus free computers?
- Would you know what to do if you lost all of your essential company data?
- Would your employees know what to do if you weren't around to advise them?
- If you trade online and your website was compromised, could you continue to trade?

If you answered no to any of the above questions then in the event of a disaster, your business may be at risk.

Description

Irrespective of your organisation's size, disaster recovery is vital to protect your business. In the event of an unforeseen problem, having a disaster recovery plan is essential. The plan is a set of guidelines to follow in the event of a problem.

If your business relies heavily on computers which became infected by a virus, a disaster recovery plan would outline where to source replacement equipment without delay, the steps your employees should take to minimise the virus spreading and what technical support would be on hand to remedy the problem.

It is a way of limiting the amount of downtime your business may suffer.

The loss of data through an accident or unforeseen incident is a common situation. Natural disasters, floods and fires could all cause businesses to lose valuable data, but an even bigger risk is presented by cyber crime. If a cyber criminal hacked your server and deleted all of your company data, or unleashed a virus that destroyed your hard disk and website, then having a disaster recovery plan is the recognised way to mitigate or limit the damage caused.



Simple steps to prevent disaster

- + Install anti-virus software and set updates to automatic to ensure that your computers and servers are protected from the latest virus threats. (see 'Viruses' flyer for info)
- + Install a firewall to protect your computer, network or server. (see 'Wireless Network Security' flyer for info)
- + Make sure all servers are housed in large fan ventilated cabinets, at least 18" from the ground with vents at the top. Never install servers or any ICT equipment in the basement. If floods occur, basements will always fill up first
- + Routers, firewalls, network switches, modems, should be on a shelf in the cabinet above the servers
- + The server's electrical power points should be close to the top of the cabinet and a UPS (Uninterruptible Power Supply) will protect your server and data in the event of total power loss
- + Formulate a disaster recovery plan. Review day to day operations then plan a way you could move to a different location and be up and running in a few hours, including short term office rental, switching IT/Telephony suppliers, informing suppliers and restoring backups etc. (see www.bcrc-uk.org for further info)

Backups

Backing up your company data is absolutely essential and should form the first part of any disaster recovery plan.

- + A backup is the term used to describe a copy of your data. It may be as simple as copying the file into another directory on the computer. The most secure way to preserve data would be to transfer the information to another type of data storage, then keep it in a secure location away from the company premises

Useful Websites

<http://www.ktn.qinetiq-tim.net/>
<http://www.berr.gov.uk/whatwedo/sectors/infosec>
<http://www.bcrc-uk.org>
<http://www.businesslink.gov.uk>
<http://www.getsafeonline.org/>
<http://www.sophos.com/security>
<http://zdnet.co.uk/toolkits/securitythreats>

Disaster Recovery / Backups:

www.zdnet.co.uk/toolkits/disasterrecovery

<http://www.howtowipeyourdrive.com> – stop data theft from old hard drives!

<http://www.preparingforemergencies.gov.uk/bcadvice/index.shtm> – HM Governments preparing for emergencies

What data needs to be backed up?

Designate a day that you will not use your computers and you will quickly measure their importance to your business. All data considered critical needs backing up. This could include:

- + All client correspondence
- + All your accounting data
- + All e-mail and e-mail addresses
- + All your database files
- + Your web site should be backed up in case the web server should fail. If it's outsourced, make sure the hosting company is making backups as they should
- + Tailored software
- + Handheld devices
- + CD's supplied with new machines should be stored safely away from the computer they refer to
- + Register all equipments make, model and serial number on <http://www.immobilise.com> which may help the Police return it if stolen
- + Install tracking software on laptops

Backup regularly – all data since your last backup will be lost so take frequent copies, even hourly, daily and definitely weekly.

Always remember to test your backups on a regular basis – companies have tried to restore data from backups only to find the data has been corrupted and if you use tapes or discs, replace them every 3-4 months.

Backup Solutions

Backed up data should always be stored in a secure location offsite. Onsite fireproof safes are often used by businesses but these also need to be data-safe and are only useful depending on the severity of the fire.

There are a number of backup technologies available:

- + Hard disk - Copying data to another computer is a quick backup technique; however, if you have a disaster you may lose all computers and all data
- + DVD – They can store around 4.5 GB of data. That's enough to store a backup for most computer users and small businesses
- + Small external tape drives - They connect via a USB port and are portable, enabling all computers to be backed up
- + Server backups. Using tapes or DVD's your server should be backed up on a daily/hourly basis
- + Online backups. Your data is copied to a remote server, initially as a full system backup then as regular smaller backups of any new data. Normally payments are made in subscription form – monthly or annually

The size of your business and its reliance on ICT will dictate which backup solution you choose.