



IT Disaster Prevention & Recovery

July 2007

Many firms just don't realise how reliant they have become on their IT systems - until disaster strikes.

Our E-Business Advisers discuss what you should do now to help safeguard yourself:

1. What are the main threats?

Firstly, many businesses rely on the data held on their IT systems to function.

For example, if your accounts are computerised or you maintain an essential customer database, you need to be aware of the risks you face.

According to American research, 60% of businesses whose IT systems are unavailable (for whatever reason) for ten days or more go bust.

Although you can easily insure against equipment loss, it's the data loss that might destroy your business if a disaster strikes.

There are several main areas of risk:

- Physical risks, such as fire, flood, lightning strike, power cuts, malicious damage and theft.
- Human error e.g. input error or careless disposal of sensitive data.
- Technical risk - for example, failure of the Internet connection could prove damaging to many businesses. Likewise, IT systems will, eventually, fail.

- IT based threats - e.g. viruses, hacking and phishing.

How much time, effort and money you need to spend on protecting yourself against these risks needs to be measured against how much disruption the threat could cause if it happened.

For example, if your business is totally reliant on your accounts system, you may wish to put stronger safeguards in place around that system as compared to another non-critical system.

Also, be aware that under the Data Protection Act you have a legal responsibility to hold the personally-identifiable data you collect in a secure manner.

You need to have a small team of people who try to identify the risks your business may face - and try to assess the impact for each risk you identify.

It is unlikely that you will be able to eliminate all risk. You should certainly have plans in place to deal with the consequences of the major ones, as well as taking steps to reduce the likelihood of these occurring.

It is much easier to prevent the problem than to try to deal with it!

Fortunately, protecting against one type of threat often safeguards you against another.

For example, taking data backups off-site, or placing them in a fire-proof safe, will help protect you against the loss of your data caused by fire, theft and lightning strike.

However - fire-proof safes are no use against



Fact Sheet

flood damage.....so you do need to assess what physical risks you face and take appropriate safeguards.

2. Protecting against risks

There are a range of practical steps you can take to mitigate risk, some obvious, others less so:

- Make sure any computer equipment is not visible from outside your premises, especially at night, to remove temptation for thieves.
- Invest in a good security alarm system
- Make sure that daily backups are taken as a matter of policy and **check that the data is recoverable and could be restored if need be!**

A backup is worthless if you can't retrieve the data.

- Give 2 or 3 members of staff this specific role - if one is on leave or ill, it then becomes the other's duty. You need to ensure that this is formalised, in order to prevent each person thinking that the other has done the backup!
- Take these backups off site or put them in a fire safe - but be aware that radiant heat can still damage backups in a fire safe if the blaze is intense enough.
- Fire safes don't protect against flooding!
- Insurance - ensure that the cover is adequate to replace equipment on a "new for old" basis.
- It is also possible to ensure against data loss - for example, after a computer failure whereby you have had to employ a specialist data recovery firm (which is not a cheap process!)

- Buy an Uninterruptible Power Supply (UPS) for your server. If the power supply fails, associated software will automatically close the server down in a controlled manner, thereby protecting your data.

- Buy "Power Surge Protection" devices for all your computer equipment, such as the PC's on users' desks etc. They cost around £25 - 35.

You plug your equipment into the electrical sockets on these devices, which then gives reasonable protection from electrical surges.

If you are in a rural area, electrical supply can be particularly problematical, and this can cause data corruption.

- Establish a strong working relationship with your IT suppliers. Be aware that their resources may be limited though, e.g. they may have to wait on their supplier before they can replace a stolen PC for you.
- Make sure your staff take care of laptops - never leave them in cars for example. They can contain very sensitive data and they are very attractive to thieves!
- Good staff training on how to properly work on IT systems can stop much inadvertent damage to data.
- Restrict access to sensitive data to staff that need to know - e.g. only allow account staff to access the accounts systems.
- If your data is particularly sensitive, use encryption techniques.
- Have a company email and Internet usage policy - e.g. don't allow Internet downloads



Fact Sheet

which might bring viruses with them.

Make staff sign to say that they have read this.

- Make sure that data is properly wiped off hard disks if you are disposing of IT equipment.

Deleting a file will not obliterate the data it contains: it is relatively simple to get this data back.

For example, this could give unscrupulous competitors great access to your customer list!

You could use special software to effectively delete any old data.

- Also be aware that there are limitations on how you can dispose of old IT equipment - the Waste Electrical and Electronic Equipment has come into force in the UK, which will prohibit just dumping old computers.

Consider donating to a charity - see Useful Links section below.

- It is vital that you install a Firewall to protect your systems from hacker attack, amongst other threats. It is even more vital if you have a broadband "always-on" connection.
- Likewise, you need to install and keep up to date Anti-Virus software to protect your business from this threat
- Phishing - the deliberate faking of emails in order to get access to information about bank account details etc - is a threat to firms as well as individuals. Make sure that staff are aware of the threat.
- Password policies - make sure that staff are aware that passwords are important, and should not be shared, or written down.

Also implement a policy of making passwords a combination of letters and numbers, over 6 characters. This makes them harder to guess.

3. Disaster recovery plan

Even though you've taken all the steps above, a disaster affecting your IT and its vital data can still strike any firm.

For example, you could still have a major breakdown of your IT systems.

If you have a well-rehearsed plan of action, worked out prior to the calamity, your business is much more likely to be able to survive with the minimum of effect.

The elements that such a plan is likely to need include:

- Who to contact - plus alternatives if that person is unavailable, on leave etc.
- What circumstances they need contacting in.
- Details of contact numbers for suppliers.
- Insurance policies etc.
- Staffing arrangements

You should test your disaster recovery plan - this might be in the form of a simple paper exercise.

In the event of a major disaster hitting the entire firm, such as a major fire, your IT disaster plan must form a part of the corporate disaster recovery plan that any business should have.



Fact Sheet

4. Useful Links

See Fact Sheets in this series on:

- “Data Protection Act 1998”
- “Internet Scams - Phishing”
- “Firewalls”
- “Viruses”
- “Hacking”
- “Spyware/Malware”
- “Internet Security - Glossary of terms”
- “Software Piracy & FAST”
- “Email and Internet Usage Policies”

Useful web sites:

www.vogon-international.com -
Vogon International is a leading specialist in data recovery and data security services.

www.itsafe.gov.uk -
Government web site with straightforward guidance on keeping your IT, mobile phones etc safe from attack.

www.donateapc.org.uk -
Matchmaking service for firms to donate un-needed hardware (computers, printers etc) to UK charities, not-for-profit organisations and educational establishments.

www.businesslink.gov.uk -
Business Link national web site, with many resources and briefings relating to business and IT disaster planning and recovery.