

**Berg Kaprow Lewis**

IT disaster prevention

Many small and medium-sized businesses rely heavily on their IT networks, but not all take adequate steps to safeguard them. System crashes, data corruption and other problems can have disastrous consequences — and could even cause a business to fail completely. To anticipate problems and minimise any damage caused you will need to set up and implement an effective disaster prevention strategy.

This briefing focuses on IT. To find out how to reduce the impact of other types of disaster, such as fire and burglary, see **Managing insurance risks**.

This briefing covers:

- Assessing the risks you face.
- Pre-empting potential problems.
- Making contingency plans.

1 Assessing risks

The amount of time and money you spend on disaster prevention will depend on what you use your system for, and the specific risks it faces. Conduct a systematic risk assessment to work out the most suitable approach.

1.1 Think about the **importance** of your systems to your business processes.

- 'Mission-critical' systems are vital to your business. They need to be highly reliable, and repaired quickly if they fail. For example, a database used by customer service to respond to telephone enquiries, or an e-commerce website.

- Accounting systems can be essential. Problems could lead to errors or delays in payment, and cashflow difficulties. You could also lose key management information.
- Other systems may be less crucial to your business. For example, if you only use a PC to write letters.

A system breakdown would be inconvenient, but not disastrous.

1.2 Consider the **value** of the data you hold. Certain types of data may be particularly valuable. For example:

- Commercially sensitive information (eg your price list or customer details).
- Personal details on employees or other individuals.

Directors' Briefing

a book in four pages

More than 160 briefings are now available.

If you need further information or help, ask the distributor of this briefing about the services available to you.

You have a legal responsibility under the Data Protection Act for how you use and protect this information.

- Information you base key decisions on.

1.3 Analyse the potential **impact** of IT problems.

- Repairing problems can be expensive.
- Delays and errors caused by IT problems could lose you customers. If customers do not receive their orders on time, they might look for alternative suppliers.

Safe system upgrades

When you make changes to your system, there is a higher risk of disaster. Following a safe procedure is essential.

A Check the upgrade is really **necessary**.

- The benefits offered by new versions of software packages do not always justify the inconvenience of upgrading.

B **Back up** the system before you start.

C Take steps to **minimise** problems.

- Make sure the upgrade is compatible with existing software and hardware.
- Wait a few months after new software is released before buying it. Problems are more likely to have been ironed out.
- Upgrade systems during an inactive period to reduce disruption, for example overnight or at a weekend. But bear in mind support may not be available at these times if things go wrong.

D Be particularly careful with **complex** changes or highly sensitive systems.

- Maintain the old system while the new one is 'run in'.
- Initially install software or equipment on an isolated part of the system only.
- Run tests to see what problems occur. Use existing, rather than new, data to make tests as authentic as possible.

E Get help if an upgrade **does not work**.

- Call the manufacturer's help desk, or visit its support website.
- Discussion groups often provide links to useful sources of information.
- If these steps do not solve the problem, get help from a local IT specialist.

- Time will be wasted correcting errors and restoring customer goodwill.
- Employees are likely to be less productive.

1.4 Identify specific **risks** faced by your system. How likely are they to occur?

- User error and power cuts are the most common problems.
- Viruses are an increasing threat if you use email and the Internet.
- Theft, fraud and hacking can be a serious risk, particularly for companies that hold sensitive types of data. For example, if you collect customers' credit card details through your website.

- IT systems also face physical threats (eg fire and water damage). See **Managing insurance risks**.

1.5 Take steps to **minimise** these risks (see 2–7).

Review the risks regularly to monitor changes in the importance of your data and systems.

2 Sensible purchasing

2.1 Look for **reliability** and simplicity when buying computer hardware and software.

- Unless you have complex IT needs, use off-the-shelf products with a proven track record. Getting support will be easier than with a bespoke package.
- Get recommendations from contacts with similar needs.
- Tell your supplier how you intend to use software, and state what other software packages your system is running. Different packages may not work well together.

2.2 Purchase the **support** you need. Depending on your in-house resources, this may include:

- Installation, configuration and any customisation needed (see 3).
- Maintenance (see 4). If you have a network, you will probably need on-site support for your servers and network equipment.

- Training (see 5.1).

2.3 Check what **guarantees** you have.

- Find out how quickly equipment will be repaired or replaced if it goes wrong (see 7.4).

“Imagine your business as a ‘house of cards’, with each card being a critical business function or process. Which cards would cause the whole structure to collapse if removed? These are the critical processes you must protect.”

Noel Carey,
IBM Business
Continuity
and Recovery
Services

“According to an American study, 60 per cent of companies whose main IT system fails for more than ten days go bankrupt.”

Steve Johnson,
Developing
Futures

“If you're using a bespoke IT system, make sure you're not dependent for support on the company which built it. You need access to the developer's password in case they are no longer available when a problem arises.”

Peter Heskett,
Harwood IT

3 Setting up your system

3.1 Design your network with disaster prevention in mind.

- Isolate any sensitive areas of the system (eg accounts).
- Install recognised anti-virus software, and update it daily using patches from the manufacturer's website.
- Use surge protectors or uninterruptible power supplies (UPS).
Set up a UPS to shut down your server automatically if the power fails.
- If your system is connected to the Internet, you should install a firewall.
See **Security and the Internet**.
- Maintain a list of each PC's configuration settings to make replacing or reinstalling your system easier.
- Consider installing a RAID system of multiple hard disks to keep key systems running if one hard disk fails.
The more computers you connect to your network, the greater the damage a system failure could cause.

3.2 Install and configure software carefully.

- Ban employees from installing unnecessary software, which could slow your system down or carry viruses.
- Check new software does not conflict with any other software you use.

In-house expertise

A Make an **individual** responsible for managing your system. This person should:

- Recommend purchases and liaise with suppliers.
- Install and configure software and new equipment.
- Provide IT support to employees.
- Keep a log of problems, and how they were solved, to help you identify and deal with recurrent issues.

B Make sure this employee knows when to refer issues to **external experts**.

- Unskilled attempts to fix problems may make matters worse.

C Give this employee appropriate **support** and training, such as freedom to contact suppliers for help or technical training.

As a minimum, read the software's 'readme' file before installation.

- Restrict installation and configuration to approved (if possible, expert) personnel. You should have no major problems with software pre-installed by a reputable supplier.
- Configure software consistently across your system.
- Run the same versions of software on all computers to ensure files are compatible.

3.3 Set up a logical **filing** structure (see **Filing and records management**). This should:

- Allow employees to find data quickly.
- Make it easy to save files correctly. Otherwise, different versions of files could be stored in different locations, with no one knowing which one is correct.
- Prevent any unauthorised access and amendments to key information.

4 Maintenance

4.1 Implement good **computer hygiene** procedures. You should regularly:

- Clean equipment.
- Run system utilities to 'clean' hard disks.
- Weed out or archive old files (eg temporary Internet files).
- Ensure your anti-virus software is kept up to date. For maximum protection check your system occasionally with different anti-virus software.

4.2 Update software or hardware, following a safe procedure (see box, page 2).

- Software patches and updates are usually available from the manufacturer's website.

4.3 Routinely check system **performance**.

- Qualified personnel can run system diagnostic tools.
- Get employees to report any problems, and investigate them thoroughly. Apparently trivial problems may be an indication of more serious, underlying weaknesses in your system or procedures..

5 Procedures

5.1 Train employees on how to use the system correctly.

“For most organisations, a disaster or crisis isn't unexpected, simply unplanned — the key to survival is having a plan and knowing it works because you've tested it.”

Kim Farr,
Developing
Futures

“Beware of 'guaranteed response times' when choosing IT support. An engineer may arrive quickly, but won't necessarily fix the problem.”

Paul Tarbox,
Vantage
IT Solutions

Most computer problems are caused by employee error.

- Give employees adequate training before they begin to use the system.
- Explain and enforce procedures for using the system.
- State who is responsible for backing up data (see 6).

5.2 Establish appropriate **security** procedures.
See **Security and the Internet**.

5.3 Set out, and implement, a clear **IT policy**.
Refer to the policy in your employment contracts.

- State what you consider to be unacceptable use of your systems.
- Specify which tasks should only be carried out by qualified personnel (eg software configuration or using diagnostic tools).
- State what kind of problems employees must refer to someone else.
Simply rebooting a computer when it crashes may provide a temporary fix — but you will not find out the root cause.

5.4 Review your **procedures** regularly.

- Employees may ignore long-winded procedures if they find a shortcut.
- Routine warning messages tend to be ignored over time.

Encourage employees to report any problems and to make suggestions for improvement.

6 Backing up

6.1 Set up an effective **back-up procedure**.

- Choose a back-up system that is easy to manage and operate, with sufficient capacity to hold all your data. Most servers designed for small businesses have a built-in tape drive for back-up.
- Make two employees aware of the back-up procedure and rotate responsibility between them.
- If using tape, have a different tape for each day of the week and keep back-ups securely, off-site.
Remember that back-up tapes may contain confidential information.
- Take one tape out of the cycle (and replace it) every month, and store it off-site for three to 12 months, so you can restore any files that go missing.

- Consider installing removeable 'swap' hard disks as an alternative to back-ups.

6.2 Test all your back-up systems regularly.

- Conduct tests to make sure you can restore data from the back-up.
- Use software which tells you the cause of any problems arising during back-up.

Get those responsible for testing back-ups to report to you once a quarter.

7 Planning for the worst

Put contingency plans in place to minimise disruption in the event of a system failure.

7.1 Provide **contact details** for sources of help.

- Usually, this will be a nominated individual. Ensure there is cover if this person is away.
- More complex problems may need to be referred to suppliers, particularly if they are providing a support service (see 7.4).

7.2 Keep original **software** secure.

- Store software disks off-site, or in a safe.
- Keep an up-to-date log of all installed software. Note which version of each package you are using, and record configuration details.
- Keep copies of any patches and upgrades.

7.3 Keep any spare **hardware** and consumables you might need.

- Old computers can provide short-term cover if newer equipment fails.

7.4 Build a good relationship with a **local supplier** or **repair company**.

- Pick one that understands your needs.
- Check equipment will be repaired or replaced quickly enough.

7.5 Make sure employees know **how to cope** when the system is down.

- Detail any special tasks they must perform.
- Put appropriate manual systems in place. For example, print out the key elements of your database so you have a back-up.

7.6 Consider **insuring** your system against the costs of breakdown and data loss.

Expert contributors

Thanks to **Bill McTaggart** (Galatea Training Services, 01484 686343); **Paul Tarbox** (Vantage IT Solutions, 01296 668966); **Peter Heskett** (Harwood IT, 020 8255 0077); **Noel Carey** (IBM Business Continuity and Recovery Services, 01926 464103).

Further help

There are other Directors' Briefing titles that can help you. These briefings are referred to in the text by name.

© Business Hotline Publications Ltd 2005. ISSN 1369-1996. All rights reserved. No part of this publication may be reproduced or transmitted without the written permission of the publisher. This publication is for general guidance only. The publisher, expert contributors and distributor disclaim all liability for any errors or omissions. Consult your local business support organisation or your professional adviser for help and advice.