CONTINUITY ERRORS

Does your firm have an adequate disaster recovery plan? **David Taylor** explains why it needs to encompass not only IT but a lot more besides.

Disaster recovery (DR) and business continuity (BC) are often seen as IT issues. Traditionally, if there was a major systems failure, the IT department had a DR procedure to restore them, and when people considered business disruption they usually thought of a hardware or software crash. Increasingly reliable hardware has since cut failure rates and made much of the back-up equipment redundant. It's now rare for a firm that has invested in the right hardware to suffer a breakdown that affects its operations. Software failures do still occur, especially when things change – during upgrades, for example – so it's important to have testing, back-ups and implementation plans in place. But falling hardware costs make it more viable to have a separate test system, perhaps also acting as a standby.

The main risk of IT failure now comes from the internet, where the threat of hackers, spyware and viruses eclipses all other issues. There's a constant game of catch-up between those developing the mal ware and those who produce detection and cleansing programs. Even if the danger cannot be eliminated, appropriate security software and devices can minimise it.

Core IT problems are, therefore, becoming less likely to interrupt your operations, leaving the most likely culprits as utility services failures, fire and theft. Although the threat of terrorism generates a lot of media attention, an attack is statistically far less likely than an extended utility service failure. Consider the impact that even a one-day power cut would have on your business.

Most people now understand that the IT disaster recovery process cannot be isolated from the core business activities. There are many organisational issues to be considered in the IT recovery plan. If several systems fail, which ones should be

WHY HAVE A DR/BC PLAN?

- 80 per cent of businesses that are affected by a major incident are forced to close within 18 months.
- 90 per cent of businesses that lose data as the result of a disaster are forced to close within two years.
- 58 per cent of UK organisations were disrupted by the attack on the World Trade Center on September 11, 2001. One in eight was seriously affected.

Source: London Prepared.

Illustrations: Steve May

restored first? How quickly does the business require the various systems to be available again? IT staff can adapt back-up methods accordingly, putting in place relatively cheap, slower recovery methods for non-critical systems and spending more on "hot standby" systems in high-priority areas.

You also need to consider whether your firm could continue operating if it were to lose the contents of its offices in a fire. Do you have insurance cover, customer contact details, headed paper, essential office supplies and other premises available at short notice? These issues aren't part of an IT recovery plan, but they are a key part of business continuity.

What should I do?

As a first step, every organisation needs proper insurance and physical monitoring. Your policy may cover fire and theft, but how about flooding? You might think that you don't need this cover if you're on the first floor – but the tenant on the second floor may have a toilet or kitchen directly above your server.

You can fit a variety of devices to help prevent disasters from striking in the first place. The most obvious of these is a burglar alarm. If you tell your insurers that you have an alarm, you must ensure that it's used correctly, since they may refuse to pay out if it emerges that someone forgot to set the system when rushing to the pub on Friday evening.

The next step is to have a written plan. The IT plan will go into technicalities and should be a separate section within the general BC plan. Both should use scenarios to generate discussions on preparing for a range of problems. IT may play a key role in the BC plan, but the IT department shouldn't "own" it. This should be allocated to a business manager who should be responsible for updating and testing it, as well as for communicating its requirements. An excellent BC plan is useless if no one knows where it is or what its contents are.

The BC plan should cover issues such as:

- What is expected of the IT recovery process – specifying systems and schedules.

USEFUL WEB SITES

Monitoring
Environmental monitoring: www.availability.sungard.com/United+Kingdom/Services/Monitoring+Services/Overviews.htm
Systems monitoring: www.halcyonsoftware.com

Recovery companies
ICM: www.icm-computer.co.uk
NDR: www.ndr.co.uk

Managed services
Anti-virus and anti-spyware: http://eu.shopmcafee.com
Anti-spam: www.messagelabs.com
E-mail: www.fasthosts.co.uk/email
HR: www.vizual.co.uk/hr_net.asp
Managed IT: www.dgt.uk.net/services.php

Remote back-ups and storage
Off-site back-ups: www.depositit.com
Off-site storage: www.ironmountain.co.uk

Planning
Business Continuity Institute: www.thebci.org
Insight consulting: www.insight.co.uk/bcm
London Prepared: www.londonprepared.gov.uk/business/businesscont
MI5: www.mi5.gov.uk/output/Page267.html

- How to order – and pay for – replacement IT equipment, software, stationery, temporary staff etc at short notice.
- How to contact all staff.
- What the business objectives are during the recovery period. For example, will you aim to trade at a reduced level, servicing existing orders and fulfilling obligations, or will you need to trade as normally as possible and pursue new orders?

Practical steps

Back up your business information regularly and keep it away from your main premises. Keep a box of essentials – for example, stationery, printed lists of information such as staff phone numbers, customers' and suppliers' contact details and bank information. Store it in an easily accessible location away from your main place of business and update it regularly.

Keep clearly written manuals for all key operations. If Adam in accounts always runs the end-of-month payroll and no one else knows how to do it, how could someone else cover his work in an emergency?

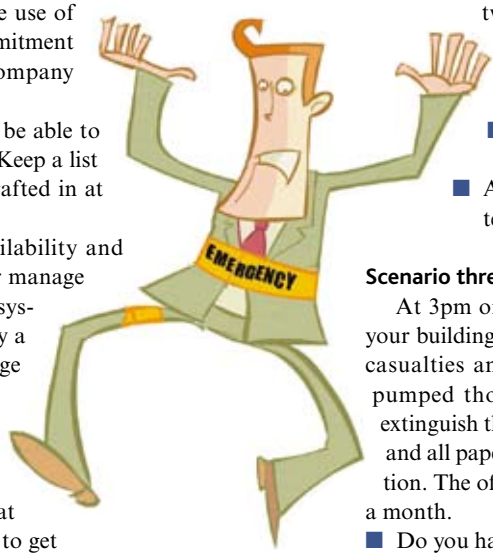
Keep a list of companies that will supply temporary staff, IT equipment and other things that you may need at short notice and, if possible, those that will accept verbal instructions without a written purchase order if you don't have headed paper or a fax machine to hand.

You may be able to find another firm that's willing to enter a reciprocal BC agreement. If you have an emergency, this company will give you some office space and the use of phones and computers in return for the same commitment from you. Obviously, it is unwise to choose a company located very close to yours.

Smaller companies in particular may need to be able to access extra workers to get them through a crisis. Keep a list of freelance or temporary staff who could be drafted in at short notice.

Managed services may improve your IT availability and recovery time, since you do not need to house or manage the systems providing the service. Back-ups, HR systems and even e-mail can be remotely hosted by a specialist provider. If you have limited IT knowledge or resources, a complete managed service may be a suitable option.

To check whether your BC plan is viable, or to start your own plan, write down a few disaster scenarios of varying severity and work out what your response would be. Here are a few examples to get you started.



Scenario one

At 6am on a Tuesday morning a tanker spills toxic chemicals in a street near your office. Your building is in the evacuation zone and the police will not allow anyone through their cordon. Your staff cannot reach the office and no one knows how long it will take to clean up the spill.

- Can you access all your staff contact numbers?
- Do you have an assembly point outside the cordon?
- Can you work by logging into your systems remotely?

REAL EMERGENCIES

If you believe that the kinds of scenarios I have described couldn't happen to you, think back to some of the major incidents of the past few years. Try using any that generate media coverage in future as scenarios to test your BC plan.

- **August 14, 2003**. Most of North America suffers an electricity blackout. Losses are estimated at $6bn. Power is not fully restored for five days.
- **February 12, 2004**. A BT control card failure cuts off 70,000 broadband users in north-west England and the Midlands from 9.30am until 4.30pm the following day.
- **March 29, 2004**. A fire damages a main BT cable in Manchester, leaving about 130,000 homes and businesses without a phone or internet connection. Half of these still have no service several days later.
- **December 11, 2005**. An oil depot explodes in Hemel Hempstead. Several nearby offices are hit so badly that all of their windows are blown in. If the explosion hadn't occurred before normal office hours, there would have been serious casualties.

These are some of the incidents that made the headlines. Many less dramatic disruptions happen every day.

Scenario two

You arrive at the office to discover that overnight roadworks have cut through a major power cable in your street. The electricity company estimates that power will be restored in about two days. You may have no working computers (and, therefore, e-mail), phones or fax machines.

- Could your business be out of touch this long and survive?
- Do you need to inform your key customers or all of your customers?
- Are their contact details only on the computer systems that you cannot switch on?

Scenario three

At 3pm on a Thursday afternoon there is a serious fire in your building. The premises are evacuated successfully with no casualties among your workforce, but the fire brigade has pumped thousands of litres of water into the building to extinguish the blaze. Most IT and communications equipment and all papers have been destroyed as a result of this intervention. The office space is unusable for at least a week, probably a month.

- Do you have alternative office space?
- Is all your company information backed up and stored away from your building?
- Can you easily restore your backed-up information?

For a more structured examination of your organisation's BC plans, try the ten-minute assessment on the London Prepared web site (londonprepared.gov.uk). FM

David Taylor spent many years managing IT at banks in the City of London before becoming a director of IT business services firm DGT Technology (www.dgt.uk.net). DGT also runs courses on how to manage IT in firms (www.itmanagementcourse.co.uk).