Business Continuity And Disaster Recovery

A bomb, fire or flood could irreparably damage IT systems and paper records simultaneously, and perhaps also destroy your building. Business Continuity Planning is a process whereby risks are evaluated and plans made to enable the company to continue operating if the worst happens.

By David Norfolk

A common misconception is that Business Continuity Management is basically a posh name for backup and recovery, needed in order to justify the enormous fees external consultants can charge for setting up a few backup jobs. However, Business Continuity Management is actually a lot more than that - or should be - although a resilient storage management strategy may well be part of it.

Peter Barnes, a practitioner in the field and General Manager of International Operations, Survive Limited, defines the concept as follows: "Business Continuity Management is the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise."

This brings out the key point - that business continuity is about keeping the business as a whole going, come what may. If you're tasked with implementing a proper business continuity strategy, you, and the people helping you, are protecting your own jobs in the event of some unexpected contingency, as much as protecting your employer from disaster.

Board-Level Support

This article is aimed at technicians, but business continuity is not just a technical issue. Getting the database and network back online is necessary, but it is far from being the only concern.

Designing (and testing) a database recovery strategy isn't that difficult. The hardest part is ensuring that procedures are followed and that some backups are stored offsite. However, if your customers can't get through to the company on the phone after a disaster they'll assume you're no longer in business and start talking to your competitors - and a proportion won't come back.

If your salespeople don't have access to a phone and a fax machine, as well as to the company database, then you may be out of business anyway, even if people are coming in to work. Of course, you may not realise this for a few months, until the impact of missed orders and an impression of unreliability does its work.

So, any business continuity strategy should be business-oriented, and must have buy-in from the business. The project should probably be led by a business manager and driven from Board level, and must have a proper budget. If it is given to a junior technician to deal with in his or her spare time, it isn't going to be effective in its prime objective: to keep the business operating, no matter what.

Selling The Idea

The first stage in planning for business continuity must be to sell the idea to the Board, if the idea didn't originate there. You may need to illustrate your proposal with some examples (see Further Information).

By all means use the World Trade Centre (New York, 26/02/1993) and the Bishopsgate Bomb (London, 25/04/1993) as examples - a lot of banks started taking business continuity seriously for the first time after those - but don't stress high-profile terrorism. Some continuity risks are far more mundane: the power lines failing, for instance, when the guy in charge of the backup generators is on holiday and no-one has documented how to switch them on.

One company is said to have been sued for US$600m after losing its processing capability for only four hours - because it missed a contractual obligation. And, once you've had your catastrophe don't assume you can't have another - in 1991 the Union Bank of Finland lost its systems due to a flood caused by a fractured mains water pipe, and then an unrelated problem

> *"Analysing risk starts with documenting threats to these processes, their internal vulnerabilities, and the consequences of various failure scenarios."*

took out a key disk drive in their AS / 400 computer before recovery was complete. As that problem was finally overcome, a power drop followed by a major surge (caused by an unnoticed problem with the flood recovery) took out all the uninterruptable power supplies, two disk drives and a processor.

Maintaining business continuity is not about reacting to one-off "acts of God", but about creating and maintaining documented procedures to cope with everything from the mundane to the seriously weird, no matter when it chooses to manifest itself.

What you need from the Board, as evidence of its commitment, is someone with the necessary responsibility and authority who is tasked to deliver the business continuity strategy; a budget; and some assurance that staff in all departments will be required to co-operate. If you can't get this it's simply not worth proceeding.

BIA

The next stage is usually to prepare a Business Impact Analysis (BIA). This involves identifying the key business functions of the organisation - those that are essential to being in the business you're in, those that generate the most profit, and those that involve regulatory or contractual obligations. The method for this is usually to visit the middle management in all the departments in the company and collect information on a form on what is critical to their function.

The interviewer must take an active part and draw the interviewee out, but she / he mustn't necessarily take what they are told at face value. It is up to the interviewer to ask the right, and sometimes the difficult, questions. You should consider the total loss of their department from something like a bomb under the departmental manager's desk - less extreme contingencies can be assessed "pro rata". You need to know about:

- The impact to their particular business function of such a total disaster.
- The priorities for recovery - which areas must function uninterrupted by the disaster.
- Infrastructure and human resources requirements for a phased recovery - highest priority areas first.
- How prepared the department currently is for such an event.
- The level to which current operational procedures are documented, and whether they are effective (if the department doesn't operate effectively when there isn't a disaster, any plans it produces for recovery may be flawed).

BIA is a highly skilled operation, and there is far more to it than is covered here. You need considerable detail, and you need to know when the interviewee doesn't know about or doesn't understand some issue and is just volunteering an answer in order to avoid looking ignorant. You need a lot of detail but, at the same time, you can't afford to waste people's time. It may well be worth your while to get external help with BIA, as long as it has a skills transfer component. At the very least, you should invest in BIA training.

Risk Analysis

Once you know which the critical systems and processes are, you're in a position to carry out a risk analysis (some practitioners put this stage ahead of BIA, but if you do that you risk wasting time on threats to non-essential systems). Make sure that your BIA, and your risk analysis, isn't limited simply to automated processes - business continuity is a "whole systems" initiative, and there is little point in recovering an automated process if the manual processes which feed it, and act on its outputs, are no longer operating.

Analysing risk starts with documenting threats to these processes, their internal vulnerabilities, and the consequences of various failure scenarios. At the end of this you can estimate how likely the various disaster scenarios are and concentrate on controlling the impact of the most serious ones.

For instance, terrorism has had a very high profile in recent years, so some companies have put vital computer resources in the basement where, presumably, they are less vulnerable to bombs. However, a little research will show that most business continuity plans are activated by fire or flood (and the normal reaction to fire ensures that you'll probably suffer a flood, too). Since water flows downhill, this makes the basement a very bad place to site critical electronic equipment.

Risk analysis is not easy. In essence, you are trying to place a quantitative value on risk by producing some function that combines the likelihood of something happening with the impact (converted to cash equivalent) if it does. You then decide on some point on the scale between "major impact and very likely" and "minor impact and unlikely" where you just accept the risk.

However, you are dealing with

> *"A Business Impact Analysis (BIA) involves identifying the key business functions of the organisation - those that are essential to being in the business you're in, those that generate the most profit, and those that involve regulatory or contractual obligations."*

Business Continuity

> *"Don't overlook command and control; when disaster strikes, you can't afford arguments about who is in charge or waste time checking with the Board that you're actually allowed to pull down that wall in order to get at the backups."*

small uncertain numbers (just how likely is it that a Boeing 747 will hit your office?) and large uncertain impacts (just how much damage does a 747 strike do, and is it the same every time?) and multiplying the two together, so don't delude yourself that your quantitative risk ratings are very accurate. One way of performing a risk analysis is to use a software package with a database of historical threats and vulnerabilities - but make sure that the database is relevant to your environment (location) and your industry.

Planning Continuity

After BIA and risk analysis you can start planning for continuity in earnest. A business continuity plan has several components. For a start, it must document the membership of the emergency response team - who is responsible for "command and control" and who will be responsible for the hands-on tasks involved in recovery.

Don't overlook command and control; when disaster strikes, you can't afford arguments about who is in charge or waste time checking with the Board that you're actually allowed to pull down that wall in order to get at the backups. During emergency recovery you need something like military command structures, and you need to be able to rely on the decisions made onsite.

Pulling down a wall and destroying your building is not such a far-fetched scenario because, after a fire or explosion, it's quite likely that the authorities will not allow you into your building, even if it is apparently undamaged, to collect such things as backup tapes. Bulldozing your back wall and dragging out the media safes with a crane may be your only option for timely recovery, and if it is necessary you probably won't have time to call a Board meeting to discuss the options. Of course, once you've thought about that scenario you'll probably decide in advance that some procedurised scheme for offsite storage of recovery resources makes sense.

This highlights another option for business continuity planning - setting up role-playing games to explore likely (or even unlikely) scenarios may make it easier to formulate plans which actually work in practice. For instance, as well as PCs and functioning databases, business continuity will require some basic facilities - desks, chairs, phones, fax machines, toilets and so on. Anything you've missed should become apparent during role-playing.

You can rent "hot site" offices, specially designed to swing into action complete with IT infrastructure if you lose your premises, and they're a very good idea. However, such facilities are usually over-allocated, on the principle that not all the clients will have a disaster on the same day. It is worth checking that the other clients don't share the same threat profile as you - and don't come from the same place.

Another tip is to document plans in terms of roles. You may need a database recovery expert with skills in DB2; document this role, but don't simply document a requirement for Bill Bloggs the DB2 whizz, as when disaster strikes he may be on holiday, or dead. Against each role, of course, you'll need a list of potential occupants, alternative occupants and possibly even external contract agencies, together with their contact details. It's also important to ensure that recovery personnel are aware of their responsibilities, and you should make sure that the possibility of being given responsibility for business continuity is made clear in contracts and induction courses.

Post-Recovery

Obviously you will document a recovery process. However, don't overlook the post-recovery clean-up. What can you salvage from the wreck? How will you handle any insurance claims?

Some of the insurance issues aren't as simple as you'd think, particularly as you may have to prove that you

> *"Maintaining business continuity is not about reacting to one-off "acts of God", but about creating and maintaining documented procedures to cope with everything from the mundane to the seriously weird, no matter when it chooses to manifest itself."*

used basic industry "good practice" to control risk and minimise your claim. Some things aren't obvious: for instance, you probably can't claim for the cost of replacing lost or damaged software, just for the cost of getting replacement disks. After all, you don't own software, you lease it, so if it disappears it is reasonable to expect the vendor to replace the distribution media at cost (but check this out in advance).

Your continuity plans will be easier to maintain and manage if they're stored in a database, and you might want to look at specialised products like the Living Disaster Recovery Planning System (LDRPS) from Strohl Systems (**www.strohl-systems.com**). One of the advantages of LDRPS is that it uses an ordinary Access database and links to Microsoft Office (rather than using its own proprietary technology), and good-looking, professional reports and questionnaires will help you get continuity planning taken seriously.

However, if you do use computer assistance for your plans, make sure that you can still get at the plans (or perhaps even a paper copy) if a disaster takes out your IT systems.

Issues When Planning

There isn't much to say about the detail of continuity planning - presumably, once you've identified the critical systems, the details of recovery will be systems-specific. Nevertheless, there are some general points to make.

Firstly, the resilience of critical systems should be designed in, not bolted on. If you know that a new system is business-critical then design resilience in from the start, in conjunction with the business - don't wait for the business continuity team to come to you. At the same time, the business analysis done for continuity planning may be useful for systems design. Make sure that it is a shared information resource as far as is possible.

However, don't overlook security. Although information about system criticality and threats is useful outside the business continuity team, it shouldn't be available to all and sundry.

Similarly, don't overlook security during business recovery - you may need to switch off some controls in the face of greater risks (such as missing contractual obligations) but this should be done with your eyes open. Consider security during the planning process and make decisions about what controls can or cannot be switched off, and why, in advance. If you don't take this approach you may find criminals engineering disasters just so they can compromise your system's security.

Most importantly, don't overlook people issues: food, sleep, health and safety regulations, and stress management. Never forget that, however well you plan, when the disaster occurs you'll be depending on your staff acting beyond the call of duty. They'll have to make difficult decisions under stress. Make it easy for them, and remember to be grateful when they pull the company's fat out of the fire.

Finally, don't overlook testing, role-playing in the early stages of planning, and simulations of real contingencies once you've finished. If you don't test your business continuity plans regularly, you can't rely on them.

Conclusion

In this article we have only begun to discuss the issues involved in business continuity management, partly because so much of the detail depends on the business you're in. However, some key critical success factors are common to all business continuity initiatives:

- Get management buy-in - evidenced by the provision of adequate resources and a budget.
- If appropriate, design in business continuity facilities from the start, as a "business requirement".
- Plan "whole systems" continuity - for the business office environment as well as for IT (databases etc), and for the post-recovery clean-up and resumption of normal business as well as for disaster recovery. Don't overlook the health and safety of your staff.
- Make sure that you can get at the continuity plans even if your premises are inaccessible and the IT systems down.
- Test your plans against likely scenarios.

If you develop effective business continuity plans you're in a very strong position. Not only are you protected from "acts of God" but you can also use your ability to get back into business after a contingency faster than the competition, and thus can help build up confidence in your brand.

Further Information

Hiles 1999, The Definitive Handbook of Business Continuity Management, edited by Andrew Hiles and Peter Barnes, published by Wiley in conjunction with Survive ISBN 0-471-98622-4.

Survive is an international special interest group for business continuity practitioners, with almost 3000 members around the globe. You can find Survive at **www.survive.com**.

PCNA

The Author

David Norfolk is a freelance IT writer and regular contributor to PCNA. He can be contacted as david.norfolk@itp-journals.com.