

EDM - A Risk Management Perspective

By Glenn Sanders, BA, Dip Lib, GDDM, MBII, ARMA
Document Manager, EnergyAustralia

Introduction

This talk is really about business continuity planning, because in response to the question “should the unthinkable happen, is our critical business information safe?” I have to answer “Maybe, but that isn’t good enough”. It isn’t good enough because:

- ❑ Safe is just the start – you might have it tucked away safely, but can you get at it? Do you have the resources, the people, and the systems, to maintain your services? What priority do you have relative to other business functions?
- ❑ What do you mean by “critical”? How did you decide? Who for? Where from? Certainly *critical* is not the same as *vital*. Or is it?

The argument for EDM is that if it were only a matter of keeping things “safe”, you wouldn’t need document managers. Disaster recovery for things electronic should be more than adequately covered by the IT backup and recovery plan, and if you have a halfway decent IT section you shouldn’t try to tell them how to suck eggs. If it is just DRP, there is no place for DM. I’ll discuss in a minute why you cannot afford to be satisfied with just a DRP.

My second point is that I shouldn’t be giving this talk and it shouldn’t even be on the program, because handling electronic documents is such an everyday, ordinary, expected part of good document management, and hence part of good records management and hence part of good business, that there is nothing different or unusual about it as far as EDM is concerned –or is there? We’ll find out, because I’m going to step through how you develop a business continuity plan, and at each step ask what is the difference because of EDM, and is there anything extra or different we have to do.

So I’m not going to talk about September 11, and how EDM can help, at least not directly. That should be pretty obvious. But I am going to talk about planning for this sort of thing, while keeping EDM in perspective.

So why not a DRP?

Why not a disaster recovery plan? After all, that’s what many standards require, and NSW State Records has an exposure draft for a DRP which came out late last year. Isn’t that what we are on about?

Well, no.

The reasons are simple:

- ❑ A DRP doesn’t go far enough.
- ❑ It focuses on things that will happen rarely, so it is used rarely, and if you and your management are risk oriented, you will therefore even begrudge the time spent developing the DRP.
- ❑ It encourages people to think about documents and records, rather than services – and people.

- ❑ It encourages people to think about the nature of the disaster rather than its effect on business.
- ❑ Even the terminology is wrong because it is not positive enough.

Typically, you spend several weeks putting together a DRP (we'll get onto how in a minute). You end up with a rather large document, maybe some agreements with vendors, IT and business units. You even run some training courses so you and your team know what to do. Then you put the plan away somewhere safe, take a copy home, lodge another copy or two somewhere offsite, and get on with life, hoping that a disaster never happens. A year drifts past, maybe you drag out the plan, run through it with your team, notice that a few names and contact details are out of date, and put an entry on your to do list. A year later, same again. You just never have time to update all the details.

And then something happens. Not a 747 falling on the building, just some clown in the car park in the basement rams the wall, busts a pipe and the computer room and your secondary storage next door is knee deep in water because the sprinklers have gone off. Of course it's late Friday afternoon, you've gone home, and the two juniors who work the late shift can't find the DRP – in fact they can't look for it because the fire alarms have gone off and the building has been evacuated.

One of them rings you on your mobile but you are on the train, it will be an hour till you get home, and some of the phone numbers you need are not in your copy of the DRP because you didn't update it yet. And when you do get home, you can't find the damned thing – was it in the box under the house, or did you accidentally throw it out when you rearranged the office last year?

It gets worse from then on. You phone your boss, the Director of Corporate Services including IT. She basically tells you to go away, she's too busy getting the backup IT site up and running. In fact, she's quite rude, especially about the relative priority of freeze drying a lot of fusty old files and getting the EDM system up again, compared with trying to get the main billing system up and running by Monday morning.

The problem is, because the DRP isn't something you use often, and because it's natural to assume that it won't happen here, or at least not to you, you don't keep it up to date, and you even forget where you put it.

The easiest way to fix all this, or most of it, is to recognise that a DRP is just a subset of a far more important and useful tool, a business continuity plan.

I first came across this when I was deeply involved in setting up Year 2000 plans for a financial services organisation. We started by looking at the IT side – software (several million lines of COBOL), hardware (several hundred older PC's to be replaced) and so on, but quickly realised we had to consider other factors as well, for example:

- ❑ The building owner's computer controlled the air conditioning, the lights, security system and the lifts
- ❑ Power was at the mercy of the computerised control room of some mob called EnergyAustralia (little did I know!)
- ❑ Staff and document delivery services relied on computerised traffic control systems outside our control

I won't go on, because it got exceedingly complex. But good systems or business analysis is essentially looking for patterns, and we eventually realised that we didn't *just* have a Y2K contingency plan, and we didn't *just* have a more comprehensive IT DRP. We had a plan that covered interruptions of pretty well any sort to any of our services. It eventuated, for example, in a standing instruction to our courier company, that if they had any reason to think there was something wrong with Sydney's telecomms systems, they were to send a driver to us every two hours, at their initiative, until we said otherwise. We would pay even if there was no work.

That's just one example. We ended up with a table (use a spreadsheet or word processor) showing functions and suppliers, possible impacts (interruption, partial loss, total loss) and resulting actions. It was over a hundred pages, but for my Document Management unit was less than ten pages. All my staff got a copy, and another lived permanently in my briefcase. It became our ready reference tool, the best place to find a contact phone number or a name. We used it all the time, so we updated it frequently. It largely replaced that part of our procedure manual that dealt with exceptions. That meant the procedure manual could focus on the normal flows, and so became simpler, and even useable.

So that's why I say don't do a DRP, even if your state records office makes it mandatory. Don't take the narrow view. Do a BCP instead.

Look at outcomes and services, not causes and objects

But the Y2K project got even more interesting, and we discovered four things.

We discovered that the one thing that would stop us in our tracks wasn't the IT backup generators, or Sydney's traffic systems, it was the lifts. We could cover pretty well everything else, but an insignificant long-term failure in a lift control system was potentially as devastating to our operations as a 747 landing on the roof. The plan had to cater, not for the disaster of a plane crash, but for the impact on the continuity of our business, its operations, services, cash flow and people, of loss of access to the building *for whatever reason*. Outcomes are more important than causes.

This led on to looking at BCP with a focus on services rather than documents. In document management we don't manage documents, we provide services. What then is our role in a disaster situation, what can we contribute? What are we good at? Well, consider these:

- ❑ We know who everyone is, where they usually are located and what their function is, so we can supplement the recovery process with ad hoc information, especially when someone else's BCP hasn't been updated recently
- ❑ We are good at shipping stuff around the organisation, physically and electronically. In a recovery situation, we have the infrastructure available to move things – they might not be documents, but some PC's, boxes of letterhead stationery, backup tapes, the odd director or two – your ability to get them quickly from A to B could be a godsend. And if you can do it without fuss, because you've previously arranged to place one of your staff with a mobile phone at a desk in the corner of your storage company's warehouse, that will be even more impressive. If you have a laptop sitting on the desk, with a fax modem, scanner and a CD burner, you are even better set up to provide document-related services as well.

Assess priorities

Second lesson. Priorities: ours, and other peoples. We'd always been quite comfortable with our IT plan:

- ❑ We had a formal contract with a large IT services company to use their disaster recovery facility
- ❑ That facility was far away enough not to be affected by localised disasters around our building
- ❑ We had our software already installed and constantly updated
- ❑ We had guaranteed access to twenty desks and phones, and we had lodged with them a couple of boxes of letterhead stationery, some pens, staplers, envelopes and so on

All we needed to do was collect the latest backup tapes from the offsite store, get over to the facility, and we could keep going.

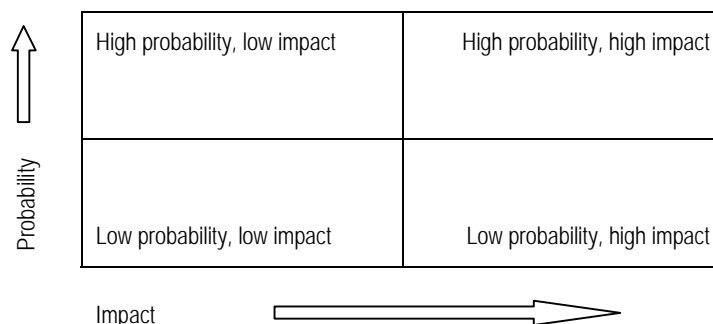
But what if we weren't the only ones? What if several buildings were affected, or, like Auckland a few years back, a whole city was down? The DR facility wouldn't tell us which other companies had contracts with them, that is rightly confidential, but it was pretty clear that any widespread disaster could well see us squeezed out in favour of much larger competitors. If every other customer has the same contract, how can you insist on priority? We tried to get a priority clause in the contract (polite smiles all round), but even if we had, a much larger organisation could have muscled in, and the DR facility would simply have dared us to sue. And what good would that have been in the middle of a disaster?

The result was that we decided to mirror some of our IT in another state, and in fact that decision ended up saving money because it worked out cheaper to run our core business systems from there, and have less essential functions, and a core systems fallback, based in Sydney. And do you think we included EDM in the list of core business systems? Ha. Other peoples' priorities impact your planning, and so do your own. As Document Managers, we have to be realistic about our place in the scheme of things. At that company, if the main billing system went down for more than three days, the impact on the cash flow meant the company became technically insolvent. EDM? Ha!

Risk-based assessment

You have to be careful with any fad. It is, for example, quite possible to define any business entirely in terms of its IT databases, or workflow, or quality assurance, or EDM. That will earn conference organisers some fees, and a few gurus will get yet another trip somewhere. But if you overstate your paradigm too strongly, and it doesn't happen to align with that of those who own the company, it won't work. It's called strategic alignment, and if you don't know what it is then we need another couple of days.

So when I say risk assessment, I don't mean whatever the latest guru happens to be spouting. To me, it is a methodology, not a message. Financial services companies are good at risk, they go to great trouble to identify risks they don't want to insure for! It looks like this:



Technically it is a scattergram, but don't let that worry you. This has become one of my favourite diagrams, along with data flow diagrams. It is a really simple way of showing the impact of something. It works wonderfully well on a whiteboard. It is not threatening. Even managers can understand it. I'm no statistician, and I can understand it. It works.

It helps you focus on the high probability, high impact risks first, followed by the low probability, high impact risks. And again, we have the difference between DRP and BCP. With a disaster focus, you look at the high impact risks almost regardless of probability, whereas with a focus on continuity, you will spend quite a deal of time on high probability, low impact issues – the everyday niggles that can blow up, or at least serve as good practice for the bigger, less frequent ones.

This sort of visual tool can also really get a workshop session going, which means I'm jumping around a bit, rabbiting on as usual, because workshops are part of step three or so in the BCP methodology. So it's about time we talked about how you develop a good BCP, and what if anything is different because of EDM. *But*, before we do, let's have a quick look at the relationship between EDM and IT.

Why not rely on the IT DRP or BCP?

This is one area where, as you get into EDM, you will find your sphere of activity changing, as will your relationship with IT. It is highly likely that they will not realise that one of three situations will apply:

- ❑ Your document management system (paper and electronic) is so good that, by definition, all IT backup files are defined as temporary working copies and are of no interest to you – this is unlikely
- ❑ Your recordkeeping system is such that the backup files are the only available copies of many records (and the IT backup schedules mean many of these are deleted illegally) – this is quite likely
- ❑ Somewhere between the two – this is uncommon but increasing

But, you say, we've all heard that a good IT backup regime will have multiple generations backups, over many months or years, with offsite storage and so on. We can use that, can't we? And they will also have DRP's in place too, won't they? The answers, in both cases, are negative.

Firstly, backup. Yes, most shops will have an adequate backup regime. But at best this can only be a part of a BCP for document management. The key point to keep in mind is that IT backup is not designed for document management, let alone records management. It is not *managed* in the way that we understand it. For example:

- ❑ There will be no correspondence between the backup schedule's media re-use pattern and your disposal schedules
- ❑ Most backup systems will only restore whole directories, not individual files, and have no facilities for guaranteeing hardware and software persistence across time
- ❑ For all your document generating software (word processors, spreadsheets, e-mails) backup is at best nightly (transactional databases may have rollback facilities); there is a possibility that documents can be created and then significantly amended or deleted in the course of a day. A good EDM system should pick this up, but a nightly backup will not.

Secondly, IT DRP's. I'm sorry, but a survey last year that you can find on the TechRepublic web site reports that the percentage of US firms with a DRP was in the low 30's. And I wonder how many of those are regularly tested, rehearsed and updated? If you have an EDM system, or even an IT system holding the database for a paper records management system, you have a right and a responsibility to ask about this, to demand to see the documentation, and to insist on regular rehearsals and updates. If you can't get a hearing, round up all the stakeholders, all your business units, and ask them to help. It is their documents you are managing, and the IT system is just the platform.

So even if you only want to do the subset DRP rather than the far-sighted BCP, you still can't push IT backup past the boundaries it was designed for. And even if your IT shop is amongst the minority that has a good DRP, it is at best a part of what you need for EDM. Your sphere of activity changes, as must your relationship with IT.

Developing a BCP

Now, pay good attention, because it gets even more boring from here on in. BCP methodology is pretty mundane, well understood, and will be familiar to anyone who has used any project or systems development methodology (DIRKS for example, one of many). It is not rocket science.

You will find references at the end of the paper to several web sites where you can find good basic methodologies. I'm going to work from that of the Business Continuity Institute, but the others are all good. Methodologies are methodologies, it's usually not important which one you use, but it is important that you use it properly.

The reason I prefer the BCI methodology is that it takes a somewhat broader view. It is concerned with business continuity management, of which the plan is just a part. They have five main stages, preceded by one that they do not number, and which I will number zero:

0. Management Commitment
1. Understanding your business
2. Developing continuity strategies
3. Developing the response
4. Establishing a continuity culture
5. Plan exercising, maintenance and auditing

Management commitment

So the first step is to get management commitment, or as the Americans call it, management buy-in. It means you have to go as high as you can, preferably to board level, to get project sponsorship and approval, a budget, resources, objectives and so on.

For document management, you may already have this step under control, as part of your established enterprise document management program. Alternatively, the organisation as a whole may be setting this up, and your role is to make sure that document management is recognised as a significant stakeholder.

So, is there anything different at this stage, just because of or for EDM? I don't think so.

Understanding your business

This stage in the methodology is key to the whole program. You have to:

- ❑ Identify mission-critical processes and functions
- ❑ Identify key external and internal dependencies
- ❑ Identify external influences that may impact on critical processes and functions

The trick is to identify all your processes, dependencies and influences *before* deciding which are mission critical. Remember the lifts! Getting agreement on this, across all business units, is no mean task. This is an area where document management may be able to assist the BCP project – if you have a well-documented functional classification and disposal schedule, backed up by interviews and so on, you may find that you can cut weeks or months off the time necessary for this stage – it’s called re-using intellectual assets. Even without this, your enterprise-wide knowledge should allow you to position yourself as a key player and significant contributor to the process.

Do not let this opportunity pass.

Once you have identified all your processes and functions, and remember that I insist that your primary focus is on those functions called services, and you have ranked them in some way (ie with services first), you can begin the business impact assessment. You look at each function, and list all the possible threats. Many threats will not need repeating for each function – if your building is inaccessible for whatever reason, it affects all functions, so after the first, you can cover many but not all others with a big “ditto”. And don’t whatever you do forget that threats and interruptions include loss of key people.

However you do it, you need some sort of scoring system, some way of quantifying the risks. This is where the scattergram comes in. You can have very complex, sophisticated scoring, or something as simple as “high probability-high impact”, “low probability-high impact”, and so on for each quadrant.

And do we have anything different here because of EDM? Are there extra things we must do to cater for EDM? Are there things that EDM can contribute over and above normal document management?

I still don’t think so.

Developing continuity strategies

This is where you work out what to do in response to each threat, and this should be a fairly fast process because you already have enterprise-wide agreement on priorities. Your options, for each threat, are usually a combination of:

- ❑ Do nothing
- ❑ Change or end the process
- ❑ Insurance
- ❑ Loss mitigation
- ❑ Continuity planning – improve resilience to interruption, recover key processes, maintain critical functions

Any strategy that requires BCP will also involve your internal and external partners, customers, suppliers or whatever. It may involve new or revised contracts, and consideration of costs and benefits of various options – a third dimension to the nice simple scattergram!

And EDM? The major difference is that if you have EDM, your services and functions will automatically be much more resilient and recoverable. I have no time for people who worry about putting things into computer system because they might lose them. The minute, the instant that something is computerised, you can have multiple copies at multiple locations at the click of a mouse.

But that's not special to EDM, it's special to anything computerised. Interrupt me if you think I'm missing something, but so far we are doing normal business practice, nothing about or for EDM makes it any different.

Developing the response

This is where the BCI starts getting firmly into disaster response, and I'm not going that way, at least not in detail. I'm committed to a continuity plan which provides for *all* interruptions, down to the level of a busted fax machine or a lost courier parcel, but we can draw from their Web site discussion a lot of response components that apply to any incident, no matter how disastrous or not it is:

- Reporting procedures, including possible external and internal communications to media, suppliers, customers
- Priorities for action eg immediate protection of people, containment of problem
- Pre-incident preparation including management authorities, roles and responsibilities
- Immediate actions (solve the customer's problem, don't look for the guilty)
- Escalation criteria and procedures
- Logging and documentation
- Possible salvage and restoration
- Orderly termination of BC process, including review and assessment

And when you write this all down, you have the first draft of your BCP. And there is still nothing special, because of or to take advantage of EDM.

Establishing a continuity culture

Plan exercising, maintenance and auditing

I'm taking these together because we are nearly finished, and you can see now that BCP for EDM isn't anything unusual or different. To implement the program, you have to:

- Select and train the various teams and participants
- Set up external relationships and internal service level agreements
- Document, document, document
- Publicise publicise publicise
- Set up BCP infrastructure – equipment, facilities
- Walkthrough, with assessment, documentation and amendment of the plan
- Define plan maintenance schedule and process

- ❑ Monitor, audit, amend, distribute, retrain etc

And you know what I'm going to say next: we still don't have anything special just for or because of EDM!

Conclusion

So there you are:

- ❑ Do a Business Continuity Plan, not a Disaster Recovery Plan
- ❑ Remember you can't rely for EDM purposes on the IT DRP or backup regimes
- ❑ Focus on services and functions, not disasters and documents
- ❑ Make it all a routine part of your everyday management, keep document management in perspective relative to mission critical functions and services, and contribute to the enterprise BCP the strengths of good document management services and skills (which in an incident may exclude documents!)
- ❑ Remember that there is nothing particularly that you should do in an EDM BCP just because your document management is electronic, nor is there anything special that EDM can contribute just because your document management is electronic. The only thing we have identified is that if you have EDM your posture will be higher, as will your responsibilities.

Useful information sources

Guidelines, standards, "how to" information

(you have to subscribe to some of these, most are mostly free)

Business Continuity Institute www.thebci.org

Gartner http://www3.gartner.com/3_consulting_services/DR_BCP/bcp.html

Knowledge @ Wharton <http://knowledge.wharton.upenn.edu>

NSW State Records www.records.nsw.gov.au

Strohl Systems www.strohl.com

TechRepublic www.techrepublic.com

Emergency Management

Emergency Management Australia www.ema.gov.au

US Federal Emergency Management Agency www.fema.gov

Disaster Recovery Companies (operating in Australia)

BMS Catastrophe www.bmscat.com

Munters www.munters.com