Disaster Recovery and Business Continuity Planning

Stewart Kidd, Security and Loss Prevention Consultant

A. Introduction

It is a maxim worth remembering that if anything can possibly go wrong - it will. Just as the toast always falls to the floor jam side down, so too can one reasonably expect the most careful of plans to come unstuck when they are put into action.

A disaster can strike any organisation, large or small. It can arrive in the shape of storm, flood, fire, a terrorist bomb, product contamination or simply a quality control failure that allows sub-standard goods onto the market. If the incident is large enough it will put the business out of action for a short or long period. Whether the business recovers or not and whether it is still operating 12 months later depends on what advance planning has taken place. This means action before and not after disaster strikes.

It has been estimated that 80% of businesses which have not thought out how they will respond to a computer disaster fail within 18 months of the incident and, of the remainder, some 50% fail within five years.

The Home Office suggests that 50% of all businesses experiencing a disaster and which have no effective plans for recovery fail within the following 12 months. To stay in business after disaster strikes requires careful pre-planning. To believe that you will easily be able to sort things out on the day will mean that your business, you and your employees will unnecessarily suffer. So a basic plan is essential and the scale of this plan will be related to the size of your business. The smaller shop holder will have a plan which can be written on one piece of paper, whereas major enterprises will have comprehensive arrangements. There is no universal solution. However all organisations, big and small, will need to go through the same basic process to produce their plan.

The biggest threats to most organisations are from fire, burglary or vandalism. Serious storms, floods or water escape from other sources can also have a major impact, especially if premises are in low-lying land near a river and important equipment, machinery or computers are sited on the lower floors. Some business are at risk from animal rights activists or terrorists because of their links with certain overseas countries. And all premises and employees are at risk, albeit tiny, from falling aircraft, chemical or nuclear pollution, disease or personal attack.

There are very few major organisations today who do not have some form of plan to deal with the consequences of an unwanted incident. However there are also very few smaller businesses which do have an effective plan. By not planning businesses, staff and shareholders are exposed to quite unnecessary risks. Planning makes a substantial difference to the possibility of surviving an incident. Indeed any organisation which undertakes a logical, structured view of the threats facing it and then works out how to respond to them has already reduced the impact if disaster strikes. If the organisation also trains and exercises its people in implementing these plans it has an excellent chance of surviving the disaster.

B. Disaster Recovery and Business Continuity

There can often be confusion - even among those who profess to be experts about the use of the two terms. Traditionally, managing a disaster has been viewed as a three part activity:

- Dealing with the actual scenario (Fire, flood, explosion, release of toxic material etc)
- Handling the by products of the disaster (Salvage, damage control, clean up, relocation etc)
- Recovery - getting back to normal business.

- Business continuity could therefore be viewed as a part of the disaster recovery plan. However many people use the two terms interchangeably. For the purposes of this paper, I shall talk about Disaster Recovery.

Disaster Recovery has always been about dealing with a single disaster or potentially disastrous situation. The definition used by many organisations is:

> *A disaster is any unlooked-for incident threatening the personnel, buildings, or normal operational structure of an organisation which is beyond the immediate ability of the organisation's staff and normal management structure to control.*

For our purposes this still serves quite well. But in 'conventional' crisis or disaster management the situation against which one plans has been more general - for example, rather than planning to deal with the specific effects of a fire, one has planned to deal with the need to relocate to a new site - thus covering with one plan, not only fire, but also explosion, flood, aircraft impact and finding one's premises inside a police cordon after a terrorist bomb explodes.

The basic principle of the plan is that it will provide a framework for you and your organisation to respond to any crisis, whether foreseen or unforeseen. Developing a library of plans for specific emergencies, and nothing more, runs the risk that the emergency which does occur is the one that was not foreseen, or that an anticipated emergency develops in ways that had not been anticipated, with the effect that the specific plans are of limited assistance or are even rendered useless.

The starting point must be the development of flexible management arrangements for handling a crisis, whatever its cause. It therefore follows that the crisis management arrangements should align with normal management arrangements, not least because normal services will have to be maintained while the emergency is handled.

This integration of routine and emergency plans and procedures embraces a number of concepts, all of which need to be embodied into your organisation if they are to be truly effective. There are four main areas where this integration must take place.

First, the principal emphasis in the development of any plan must be on the response to the incident and not the cause of the incident. Thus the plan has to be flexible; it has to work on bank holiday weekends or in freezing weather conditions. It has to be clearly written and easily understood. All involved must clearly understand the part they have to play. It will need to be regularly tested against specific circumstances. This will require an assessment of the hazards faced by your organisation and consideration of the adequacy of the planned response in each case.

Second, any emergency management arrangements must be integrated into your organisation's structure - this is particularly relevant to the selection of the emergency team. Emergency plans must build on routine arrangements and it is therefore essential for those who will be required to respond to any emergency to be involved in the planning process. This sounds like common sense. However all too often independent groups develop plans for an organisation which are only dusted off after the incident has occurred, by which time it is too late and that absolutely crucial immediate response during the 'golden hour' is less than effective.

Third, the integration of the activities of different departments within your organisation. The overall response to a crisis will invariably need input from a number of different departments. Effective planning must integrate these contributions in order to achieve an efficient and timely response to an incident. Not to be aware of the contribution to be made by other sections within an organisation is a recipe for a muddled response.

C. Risk Assessment

Although all businesses should now be used to the fact that they are required by law to undertake a risk assessment for all fire and safety related matters, the idea of assessing risk still seems to fill some people with panic.

Before making any plan it is sensible to review your loss prevention measures to see if you can spot any flaws in your organisation. Correcting these will automatically reduce the impact of a disaster as well as reducing your vulnerability to other losses. Indeed, a number of insurers are now starting to insist on this "risk management" approach as a prerequisite for insurance cover. The areas which you need to think about are:

- Financial planning;
- Computers. it and record keeping;
- Raw materials and other essential supplies;
- Customer and production records;
- Staff and personnel matters;
- Communications and PR;
- Security, fire and safety;
- Spares and maintenance.

- If you identify a vulnerable area or activity, it is often relatively cheap and cost-effective to remedy the deficiency rather than trying to plan to deal with it.

- A good example of this is when a utility company found itself facing hugely increased premiums to deal with the consequences of damage to a supply cable when crossed a channel. Ships often dragged their anchors in this area and this caused damage and loss to the supply company. The utility examined the situation and decided that it would be more cost effective to self-insure this particular risk after first stockpiling the cable necessary to remake this particular crossing. Additional measures such as improved buoyage and channel markers and a software modification to the harbourmaster’s surveillance radar (utility company funded) which meant that 24 hours worth of radar images were recorded were also implemented. So, the risk of a break was lessened but if one took place:

- The interruption to supply was minimised as all materials to repair the break were to hand;
- The cost of the break was reduced;
- There was a much improved chance of recovering all costs from the ship which could be more easily identified.

D. The Disaster Management and Recovery Plan

One thing must be understood - and while this may by now be a cliché, that in no way changes the truth: by failing to plan for foreseeable disasters, a company is clearly planning to fail.

1. Drawing up a plan

Once the objectives have been set out, work can be started on drawing up specific parts of the plan, but before beginning this task, there are a number of general points which should always be borne in mind:

a) the shorter a plan is, the better;
b) wherever possible plans should be drawn up in house (no consultant, however experienced, can understand your business as well as you do);
c) no plan can ever cover all eventualities and to try do so is counter productive.

Although all plans will be different they will have a number of features in common. The checklist below serves as an outline for those who may have to draft a disaster plan from first principles.

1. The **Introduction** will contain:
a) a clear statement of the purpose of the plan (e.g., continue normal operations, continue to operate at a reduced level; shut down activities as quickly and as safely possible, etc.).
b) a statement of intent and support by senior management.
c) a description of premises or facility and an outline of the activities which take place there.
d)The structure of the team(s) who are responsible for managing the recovery. Team Leaders should be nominated and in larger organisations there should be a nominated deputy for each post.
e) Under what circumstances the plan is to be put into action (failure in supply chain; loss of essential services, data loss; system failures, etc.).
f) Expected life of the plan (How long can operations continue in contingency operating mode?).
g) Post-plan activities:
- Criteria for returning to normal operating mode;
- Procedures for returning to normal operating mode;
-Procedures for recovering lost or damaged data.

2) The **Main Part** of the plan will contain:
- Data protection and recovery arrangements, for example:
- Procedures for back-up and off-site storage;
- Mutual aid (for example, running programs;

- Sources of replacement equipment and software.

a)Details and data relating to customers and suppliers.

b)A review of key plant or equipment, such as:

- Identification;
- Location;
- Support arrangements (ie energy supply);
- Methods of protection or replacement;
- Stockpiling or sources of spares or components.

c)Availability of transport.

d)Forecast of needs.

e)Designation of alternate sites for operations.

f)Manpower and personnel, for example:

- Details of key staff (additional or secondary skills);
- In-house fire and salvage teams;
- Sources of external assistance and mutual aid;

g)Security concerns, for example:

- Site protection (including gates and perimeter);
- Reception of emergency services;
- Assigned rendezvous points;
- Management of the media and other visitors;
- Support from local police.

3. Supporting **Annexes** will cover:

a) Communications;
b) PR and advertising matters;
c) Staff welfare;
d) Call-out sheets.

There may be other factors special to your business, and the plan should be amended when these become apparent during training sessions and exercises

E. Senior Management Support and Endorsement

The completed plan must be seen to have support at the highest level and a clear statement to this effect must be placed at the beginning of the plan. Without Board or similar support few line managers will respond enthusiastically to the diversion of resources which is implicit in developing contingency plans and training to implement them.

Experience teaches that the best way for a plan and the resources it needs to be put in place is to find yourself a ‘white knight’ at board level. In some organisations this might be a particularly appropriate role for a non executive director or outside board member.

Top management ‘sign-off’ is absolutely fundamental and without it, you will not be able to do any useful work beyond the initial planning stages.

F. Other Support Services

All plans will need to allow for the provision of specialist support and services. These will include such things as:

- Catering;
- Welfare;
- Provision of clerical support - including telephone operators;
- Other building services
- Cash/cheque disbursement.

G. The Emergency Team

There is a temptation to say that the obvious people to participate in the management of the emergency must be the Board. After all, some arguments run, they represent all facets of the company's activities, they are ultimately responsible for its performance and no one knows its strengths and weaknesses better than they.

It is suggested that this argument is deceptively seductive, for it could lure one into thinking that nothing else needs to be done after the plan is prepared. The reality is that the Board is the last group of people who should be pitchforked into managing a major emergency. This is for the same reasons that at first sight make them apparently ideal. The Board's objective is to run the company and anything which distracts them from their primary purpose must be avoided. Indeed, during an emergency, it is even more important that they must not be diverted from this. Other arguments against imposing emergency duties on Board members include oft-expressed concerns that the stresses and strains of an on-going emergency might prove too much for its older members! At least one major petrochemical company does actually utilise such criteria when selecting nominees for emergency appointments.

The ideal emergency team therefore will not contain more than one or two Board members. Most of the participants will be second-tier managers who enjoy the confidence of their immediate bosses. The ideal balance would be something like this:

- Company Secretary (Board Member) - Chairman
- Financial Controller
- Facilities Manager
- Personnel Manager
- Production Manager
- PR Manager
- Risk Manager
- Security Manager

Each team member will have a sub group reporting to him or her, for example the Production Manager's sub group could contain:

- Production Manager (Group Leader)
- Production Manager's secretary - Diary, communications and follow-up
- Finance Officer
- O&M/Industrial Engineer - Alternative Production Methods
- Purchasing Officer - Resources Planning
- HR/Personnel Officer - Manpower and Welfare

The Emergency Team with appropriate back-up would be well able to manage most situations without need for recourse to the Board - unless major expenditure is anticipated -

in that case the proposal would be taken to the would be handled by the Company Secretary - perhaps backed up by the appropriate Team member.

H. Need for Back Up - Enter the B Team

It is possible, in certain scenarios, to postulate that there might be a need for a reserve team - obviously in any emergency situation which lasts for more than a couple of days, no one could expect the team members to operate at peak efficiency. There are two possible solutions.

The one adopted by local and central governments when managing emergencies is the concept of the ‘A’ or primary team working during ‘normal’ hours. They would then hand over to a second or reserve team for the overnight period. This ‘B’ team needs to be headed by an individual with proven capabilities - in local authorities it might be the Deputy Chief Executive or Deputy Director of Administration and Finance. In the private sector the most appropriate individual might be a senior manager or director with an in-depth knowledge of the company.

I. Control Centre and Communications

Whatever the composition of the team, one thing is certain and that is the need for a suitably equipped location in which to operate.

Local authorities have the luxury of purpose built emergency centres. This is unlikely to be the case inn the private sector except perhaps for airlines and the oil industry. Despite this disadvantage there are few corporate office that cannot be converted to emergency use with a little planning and ingenuity.

The needs of the emergency centre in order of priority are:

- Communications equipment (Internal/external phones, fax, internet connection);
- Reliable power supply;
- Big enough to accommodate the whole team and support staff in relative comfort;
- Access to smaller offices for briefings, press conferences, private meetings;
- Catering and usual support facilities including toilets etc.

Communications are perhaps a primary factor in managing the emergency. Their importance cannot be over-emphasised. While mobile phones are extremely useful care should be taken not to be wholly dependent on these as in a major national emergency it is likely that the Government will switch the system off. Even in a comparatively local crisis situation the mobile phone net me either deliberately isolated as a precautionary measure. Accidental disconnection by the operating company may also take place as a safety measure

J. Training and Exercises

One of the most common failings in contingency planning is to prepare detailed plans and then sit back and assume that if the unthinkable does happen everything you will be all right.

This is a most dangerous and deceptive illusion. A paper plan on its own is worth considerably less than the effort that went into drafting it.

Training of all those who have a role in the plan is essential. This should begin with formalised sessions covering the contents and purposes of the plan until all those involved are familiar with the details. It is then appropriate to hold limited-scale exercises with individuals and groups. Once this has been achieved, at least one full scale exercise should be held at least every two years possibly involving the emergency services so that, in the event of a real disaster, they are familiar with your premises and you are familiar with the way they work.

K. Revision of Plans

Another deceptive and dangerous assumption is the idea that once a plan is written it is complete. Plans require constant reappraisal and revision as flaws and omissions in the plan will always be revealed during exercises. At the same time, changes in organisational structure necessitate regular revision and updating of the plan and, of course, more training. This training/revision cycle can be expressed in the following sequence:

a.Draft plan.
b.Formal training.
c.Limited exercise.
d.Revision of plan.
e.Full scale exercise.
f. Revision of plan.
g. Start cycle again with formal training

L. Conclusions

One of the more encouraging things about disaster management is that just by starting to plan you will automatically improve the risks of your company's survival. By assessing the risks and hazards you face you will learn more about them and be able to take simple cost effective measures to eliminate or control the hazards. At the same time, by getting the concept of crisis preparedness aired in the organisation it is likely that if something serious does go wrong the initial delays and 'freezes' which take place in such circumstances will be absent. The more used to working under such conditions people are, the more readily they will adapt to a wide range of other circumstances.

Note:

Some of the content of this paper was originally prepared by the author for the 1996 Home Office publication '*How resilient is your business to disaster ?*'