

# **Disaster Recovery**

## ***Tips for business survival***

A Guide for businesses looking for disaster recovery

November 2005



## ***Introduction***

The aim of this paper is to highlight the importance of having a robust contingency plan in place covering crisis management and disaster recovery.

It will also emphasise the importance of this plan being regularly tested and revised.

The topics in this paper are shown below: -

- Disaster recovery scene
- Disaster statistics and implications
- Disaster recovery planning
- Coping with physical disasters
- The role of the emergency services
- Recovery periods

It is hoped that this paper will provide practical advice for putting a management plan in place and will guide businesses in asking the right questions.

## ***Disaster Recovery Scene***

In 2003 over 4,000 businesses of all sizes in London were contacted by the London Chamber of Commerce and Industry to ask about their emergency plans should the business experience a fire, suspected bomb, a chemical incident or need to evacuate into a safer area.

The survey revealed that in the main, large and international businesses had contingency plans in place and knew how to use them. Worryingly smaller businesses did not seem to have any disaster recovery plans in place. Key findings were: -

- 83% of SME's in London do not have either a written security policy or contingency plan.
- 20% of larger businesses in London also do not have any written security policy or contingency.
- Only 10% of businesses with plans has tested them or trained employees in how to implement the plan

Although London businesses have been through several bombings in the 1970's and 80's the large majority of SME's in the capital do not seem to have considered the effects of an interruption to their business. If this is the case, the level of preparedness of businesses outside the capital is likely to be similar, if not worse.

## ***Disaster Statistics and Implications***

Investigations have shown that: -

- 90% of businesses that lose data in a disaster are forced to close within 2 years.
- 80% of businesses without a tested recovery plan are forced to close within 12 months of a fire or flood.
- 43% of companies that have experienced a disaster never recover fully.
- 50% of companies that experience a major computer outage will be forced to close within 5 years.

- A company that has a computer outage lasting more than 10 days will almost never recover its full financial capability.
- Less than 50% of businesses in the UK have any form of business continuity plan in place.
- Of the above 50%, only 43% of businesses test their plan annually.
- One in 500 data centres in the UK have some sort of major disaster every year.
- 45% of companies that have a crisis management plan in place do not have a dedicated disaster recovery.
- 58% of UK organisations were disrupted by the September 11<sup>th</sup> attacks in the USA, 1 in 8 were severely affected.

## ***Disaster Recovery Planning***

### **I am only a small business do I need a recovery plan?**

All businesses need to prepare a plan to cover disasters including theft, fraud, fire, flooding, IT and utility failures. Depending on the area you are based and the work you are involved in you may need to include sabotage (including vandalism) and terrorist attacks.

### **What key precautions should be taken?**

There are several key precautions that must be considered when developing your disaster recovery plan. These include: -

- Protecting people, power supplies, internet connections and key facilities. You should identify staff with first aid or other medical training. You should also keep an up to date list of contact details for all employees, including temporary workers, out-workers and any work experience students.
- Valuable documents that are easily damaged should be stored in reinforced boxes or filing cabinets. You should consider placing important paper documents in fireproof cabinets. Paper files are a fire hazard so you may want to enforce a clear desk policy in the workplace.

- Analyse which business applications and procedures are critical to the business and which could be put on hold for a period of time without causing long-term damage to the business. Remember that some less critical processes are more important than others.
- Put together a list of all business equipment, procedures, activities and skills within the business.
- Identify an [alternative business site](#) to locate staff in that is well away from the normal location (for example in the event of a chemical incident there may well be an exclusion zone set up). Make sure that the same utility companies and communication companies do not serve this alternative site as the normal location.
- Put together a list of key business operations and set daily or weekly timescales for the reinstatement of these operations.
- Ensure that staff know, and understand, that in the event of your existing premises being severely damaged that they may be required to work in the alternative location. Consider how staff would get to the other location.
- Prepare an internal emergency communications plan so that everyone knows who to contact in the event of an emergency.
- Develop an external communications policy, who will get post redirected for example. Who will contact customers and suppliers ?
- Consider conducting background checks (CRB or [disclosure checks](#) for example) on employees with access to sensitive information.

## **What other precautions should be considered?**

As well as the key precautions listed above there are other things that should be considered. These include :-

- Applying cross-training between teams in critical business areas. This is good policy anyway to ensure that more than one person or group of people know how to do a particular job in the business.

- If you have more than one department or location set up a method of "borrowing" personnel from other locations or departments.
- Publicise the disaster plan to members of staff via a newsletter.
- Consider prohibiting key executives from travelling in the same aircraft is necessary to increase the odds of business and personnel survival.

### **Do I need an emergency pack and where should it be stored?**

It is useful to create an emergency pack so that in the event of a disaster everything is in the same place. It is important that such a pack is stored **off-site** but should be easily accessible.

### **What should be in the emergency pack ?**

**Essential items** that should be in the emergency pack include :-

- The business recovery plan
- List of employees with accurate contact details
- List of suppliers and clients
- Plan of the business site (office, yard, workshop etc)
- Computer backup tapes and disks
- Spare keys
- Spare stationery
- Company seals etc

**Other useful items** (not all of these would be applicable to every business and there may be items that are not on the list your business would want) include :-

- Message pads
- Flip charts
- Charged mobile phone with available credit (some mobile phone suppliers allow you to purchase airtime that does not expire)
- Throwaway camera (for evidence of damage)
- Pens, pencils and possibly coloured chalk
- Torch / [Megaphone](#) / [High-Visibility Jerkins](#) / Spare batteries

## **How do I tell my employees about the plan ?**

If you have not told your employees about the disaster plan before it needs to be put into place it is too late.

Plans need to be carefully communicated to employees so that it does not cause undue alarm to staff. Try to explain that it is part of the planning that all businesses should undertake.

It should be remembered that plans need to be updated regularly and copies should be available to all employees, although you may want to restrict access to the contact details for staff to a smaller number of employees.

## **What could a disaster mean for my business ?**

If a disaster occurs it could mean loss of income, goodwill and image and could potentially damage the company permanently.

## **Should my business have a disaster recovery team ?**

All businesses should have a team of people that have been identified and trained in the disaster recovery team. Members of the team should be selected on their personal strengths and weaknesses and not on the job that they do, for example in the event of an emergency you will need people that will not panic and will follow the prepared plan – however if a situation develops that is not in the plan they need to be able to react to the situation.

## ***Coping with a physical disaster.***

### **What should my business do if a disaster strikes ?**

First check that all staff and visitors are accounted for and are marshalled to an external assembly point away from the building.

Establish contact with the emergency services, utility companies and local authorities as appropriate.

In the event of a long lasting disaster (e.g. not just a fire alarm) consider transporting employees home safely if necessary.

Don't panic but provide leadership and crisis control  
Talk to employees so that they are aware of plans. Ensure that all personnel from the CEO to the temporary receptionist know exactly what is expected of them in an emergency.

## ***Role of Emergency Services***

### **What is the role of the emergency services, the police and the local authorities in the event of an emergency?**

Obviously, the involvement of the emergency services will depend on the type of disaster. The minor disasters (in business terms), for example a major power failure, will not involve them at all, while major disasters such as fires may well involve all the services.

In the event of a major incident the police, emergency services and local authorities are likely to be heavily involved.

The police will ensure that everyone is in a place of safety well away from the disaster scene (be prepared to have your evacuation point moved).

The ambulance service will try to save lives, will look after the injured and will alert local hospitals to the disaster.

The fire service will rescue and save lives, fight fires, attend chemical incidents and ensure safety.

Local authorities may be involved in supporting the emergency services, co-ordinating services provided by the voluntary sector and assessing the structural stability of buildings.

## ***Recovery Period***

### **What should be in place to help a quick recovery?**

It is wise to have the following systems in place: -

- Take daily and weekly backups of computer data

- Keep the backups and any tapes, disks, original software, licence agreements and contracts (or copies of them) off site in a secure location.
- Ensure that the business has sufficient insurance cover to pay for the disruption to the business, cost of repairs, hiring temporary staff, leasing temporary premises and equipment. In the event of a disaster don't forget to **tell your insurance company immediately**.
- Watch for signs of stress or fatigue in members of the disaster recovery team. Even good members of staff reach a point where they can no longer think clearly and may make serious errors. If signs are spotted try to give the affected person some time away from the situation – don't make them feel that they are failing however.
- Put the planned communication strategy into operation to reassure key customers and suppliers that it is business as usual as soon as possible.