

*disaster recovery:
business tips for survival*

Information Centre Guide
May 2003

INTRODUCTION

Disaster recovery: business tips for survival

The aim of this fact sheet is to highlight to companies irrespective of size the importance of having a robust, fully tried and tested and regularly revised contingency plan in place covering crisis management and disaster recovery.

Disaster can strike at any time. It could result from computer hacking of a company's IT system, fire, flood, fraud, suspect explosive devices, disgruntled employees, terrorist attacks or a chemical biological incident. Research has shown that small and medium size enterprises are particularly at risk

The topics contained in this fact sheet are grouped as follows:

- | | |
|---|------------------|
| • Disaster recovery scene | Pages 2-3 |
| • Disaster statistics/implications | Page 3 |
| • Disaster recovery planning | Pages 4-6 |
| • Coping with physical disasters | Page 6 |
| • Role of emergency services | Page 6-7 |
| • Recovery period | Page 7 |
| • Support and advisory organisations | Pages 8-9 |

It is anticipated that this fact sheet will provide practical advice for putting a crisis management plan in place. London Chamber members seeking further information are most welcome to contact the Information Centre at the London Chamber on: telephone: 020 7248 4444; fax 020 7203 1863 or email info@londonchamber.co.uk

Compiled by:

**Information Centre
London Chamber of Commerce and Industry
May 2003**

Business Tips for Surviving a Disaster

DISASTER RECOVERY SCENE

More than 4,000 businesses in London were recently contacted by the London Chamber on their contingency plans should their company experience a fire, suspected explosive device, a chemical or biological incident or need to evacuate into a safer area.

The survey included the following questions:

- company security and company continuity policy in existence?
- how recently have these policies been revised and tested?
- have employees been trained on contingency planning?
- level of confidence or fear that their building might be vulnerable to terrorist or catastrophic attack?
- level of awareness on contingency planning?
- access to security and continuity planning information?

This research by the London Chamber on disaster recovery revealed a worrying low level of contingency planning by small London businesses. It found that the large and international London business community mostly had policies in place and knew how to use them. From the 4,000 London business interviewed key findings were:

- 83% of London SMEs have neither a written security policy nor a written contingency plan
- only 17% of London SMEs have a contingency or security plan in place
- only one in five of larger London businesses had any contingency or security plan in place
- 10% of the London companies having a contingency or security plan in place had tested the plan or trained employees to use the plan
- high percentage of major London businesses aware of the need for contingency planning
- 80% of large businesses in London have back up plans in place that would help them survive if they, or London, were subject to a terrorist attack.

- gap exists between a company developing plans and testing them to confirm they are workable with companies lagging behind in the training of employees

Following on from the research undertaken by the London Chamber the following disaster statistics confirm the serious implications for any business that does not have a robust and regularly tested recovery plan.

DISASTER STATISTIC/POTENTIAL IMPLICATIONS

- 90% of business that lose data from a disaster are forced to shut within 2 years of the disaster
- 80% of business without a well structured recovery plan are forced to shut within 12 months of a flood or fire
- 43% of companies experiencing disasters never recover
- 50% of companies experiencing a computer outage will be forced to shut within five years
- companies experiencing a computer outage lasting longer than 10 days will never recover its full financial capacity
- less than 50% of all organisations in the UK have a business continuity plan
- 43% of companies who have a business continuity plan do not test it annually to ensure that it works
- one out of 500 data centres experience a severe disaster every year
- 80% of companies have not developed crisis management to provide IT coverage to support business continuity to keep the business functioning effectively
- 25% of financial institutions have no business continuity plan
- 19% of financial institutions who have business continuity plans have not tested them in the last five years
- 40 % of companies that have crisis management plans do not have a team dedicated to disaster recovery
- 58% of UK organisations were disrupted by September 11th with one in eight severely affected

DISASTER RECOVERY PLANNING

Should all companies even small companies have a disaster recovery plan?

All companies need to prepare a recovery plan to cover disasters such as theft, fraud, sabotage, extreme flooding, fire, IT and utility failures and terrorist attacks

What key precautions should be taken?

- protect people, power supplies and key facilities. Identify staff with first aid or other medical training. Maintain the latest contact details on all employees including temporary workers and work experience students
- valuable documents that are easily damaged should be sorted in reinforced boxes. Paper files are a fire hazard so enforce a clear desk policy
- analyse key business applications. Identify which applications are critical to the business and which applications could be put on hold for a period of time without causing long term damage
- prepare an inventory of all business equipment, procedures, activities, skills and the intellectual capital of the organisation
- identify an alternate temporary business site to locate personnel well away from the main building and ensure that it is not served by the same utility companies or communication company as the main building
- prepare a list of key operations and set daily and weekly time scales for the recovery of these operations
- ensure that employees understand that if existing premises are severely damaged a different work location identified in the recovery plan will need to be operational
- prepare an internal emergency communications plan
- develop an external communications strategy
- consider conducting background checks on employees and periodic checks of anyone with access to sensitive information

Are there any other precautions that could be considered as part of disaster planning?

- apply cross training across all teams in critical business processes
- have a mechanism in place to borrow personnel from other departments or locations within the company

- incorporate contingency plan developments on the intranet and in monthly newsletter to keep all personnel informed
- increase the odds of personnel and business survival by ensuring that it is company policy to prohibit key executives from travelling on the same aircraft
- consider conducting background checks on employees and periodic checks of anyone with access to sensitive information

Should a company hold an emergency pack in the event of a disaster and where should it be stored?

It is useful to have an emergency pack in the event of a disaster as it can provide a business with the bare minimum to keep working. Such a pack **MUST** be stored offsite

What items should be contained in the emergency pack?

Essential items:

- business recovery plan, list of employees with contact details, IT providers, client and supplier details, building site plan
- computer back up tapes/discs
- spare keys, stationery, company seals

Useful items:

- torch and megaphone plus spare batteries, tape
- message pads and flip chart
- coloured pens and pencils, chalk
- mobile telephone with credit available
- dust and toxic fume masks
- throw away camera

How does a company communicate a disaster recovery plan to the employees?

- contingency plans will need to be carefully communicated to employees without creating undue alarm and explained as a key part of business planning

- regularly updated copies of the plan need to be available to all employees
- if a disaster has occurred it will be necessary to issue the external communications strategy document to prevent loss of customers and goodwill
- ideally educate personnel on the effects of traumatic stress and in ways to help themselves and others in a crisis

What could a disaster mean for a company?

- it could mean loss of income, goodwill, brand, image and could potentially damage the company permanently

Should a company have a disaster recovery team?

- all companies irrespective of size should have an identified and trained disaster recovery team
- select a disaster recovery team by accessing the personal strengths and weaknesses of the personnel
- ensure succession planning is prepared for all levels of personnel

COPING WITH A PHYSICAL DISASTER

What should a company do if disaster strikes?

- first check that all staff and visitors are safe and 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
- transport employees safely home where necessary
- provide leadership and crisis control
- communicate with employees so that they are aware of plans and any emergency evacuation procedures. Ensure that all personnel from the Chief Executive to the temporary receptionist know what is expected of them in a disaster

ROLE OF EMERGENCY SERVICES

What is the role of the police, the emergency services and the local authorities in the event of a disaster?

The police, the emergency services and local authorities will be heavily involved in any major incident.

The police will ensure that everyone is in a place of safety well away from the disaster scene. They will be responsible for keeping people away from the disaster scene.

In addition to saving lives and caring for the injured the ambulance service will alert hospitals to the disaster

The fire service will rescue and save lives, fight fires and ensure safety management.

The local authorities will support the emergency services and those affected by the disaster, co-ordinate the services of the voluntary sector and access the structural stability of buildings

RECOVERY PERIOD

What systems should be in place to assist with a fast recovery programme?

It is wise to have the following systems in place:

- take daily or weekly back ups of all computer data.
- ensure that any tapes, disks, software, licence agreements and contracts are located in a secure offsite location. Although this will involve extra costs consider outsourcing these IT activities to IT specialists
- maintain a strict clear desk policy as documents stored in filing cabinets can help with salvage prospects
- ensure that the company has sufficient insurance to pay for the disruption to the business, costs of repairs, hiring temporary employees, leasing temporary premises or equipment. **Report the disaster to the insurance company immediately**
- use the skills of the in house crisis management team who will have devised a plan of action
- watch for signs of excessive stress or fatigue by the recovery team. Even exceptionally good performers can reach a period where they can no longer think clearly and serious errors could be made
- identify “at risk” employees, those who are deeply affected by traumatic stress. See that they are moved to a safe environment under the care of counsellors or friends
- put the planned communications strategy into operation to minimise loss of customers and goodwill. Reassure key customers that it is business as usual as soon as possible

SUPPORT AND ADVISORY ORGANISATIONS

How can a company obtain additional guidance on disaster planning/ crisis management?

A number of organisations and websites have been identified as useful sources of information.

For London specific disaster recovery /crisis management advice contact:

Corporation of London provides contingency planning in the City of London:
http://www.cityoflondon.gov.uk/our_services/law_order/security_planning/index.htm

Corporation of London provides a free pager alert scheme. This scheme operated by the City of London Police relays, via a pager, security and crime related information to business in the City of London.

http://www.cityoflondon.gov.uk/our_services/law_order/security_planning/keeping_you_informed.asp

<http://www.pageralert.co.uk/>

Corporation of London provides a free security email service which circulates via email information regarding events in the City that may affect the security of City businesses and their employees.

http://www.cityoflondon.gov.uk/our_services/law_order/security_planning/keeping_you_informed.asp

London Resilience - this site signposts all London front-line organisations
<http://www.londonprepared.gov.uk/>

Business Link for London advises on disaster recovery planning:
<http://www.bl4london.com>

For specific disaster recovery advice contact:

The Home Office – covers terrorism:
<http://www.homeoffice.gov.uk/terrorism/>

The Home Office also provides a handbook for managers on maximising business resilience to terrorist bombings:

<http://www.ukresilience.info/contingencies/business/business.pdf>

Civil Contingencies Advice to Business. This is the website of the Civil Contingencies Secretariat in the Cabinet Office and provides links to a series of documents designed to aid businesses in continuity planning:
http://www.ukresilience.info/contingencies/cont_bus.htm

This site indicates how resilient a particular business is to disaster.
<http://www.ukresilience.info/contingencies/business/resilient1.htm>

UK Trauma Association advises on post traumatic stress disorder:
<http://www.uktrauma.org.uk/>

For specific advice on bioterrorism contact :

City of London for advice to businesses on chemical or biological attack:

http://www.cityoflondon.gov.uk/our_services/law_order/security_planning/chemical_biological_attack.htm

Health and Safety Executive for guidance for businesses on handling mail:
 Biological/Chemical Threats by post:
<http://www.ukresilience.info/package.htm>

Health and Safety Executive for issues on the control of major accident hazard regulations (COMAH):
<http://www.hse.gov.uk/hid/land/comah/notif1.pdf>

Faculty of Occupational Medicine for sources of information on bioterrorism:
http://www.facocmed.ac.uk/content/cbrnt_links.htm

Department of Health for briefing notes for the public on biological chemicals and diseases:

Anthrax <http://www.doh.gov.uk/epcu/cbr/biol/anthbriefpub.htm>

Botulinum toxin <http://www.doh.gov.uk/epcu/cbr/biol/botbriefpub.htm>

Plague <http://www.doh.gov.uk/epcu/cbr/biol/plagbriefpub.htm>

Smallpox <http://www.doh.gov.uk/epcu/cbr/biol/smallbriefpub.htm>

Ricin DoH Guidelines http://www.londonprepared.gov.uk/ricin_guidelines.pdf

Ricin Q&A <http://news.bbc.co.uk/1/hi/health/2636105.stm>

Disclaimer

Whilst every effort has been made to ensure the data published in this Guide is accurate, the London Chamber of Commerce and Industry cannot accept responsibility for any errors or omissions. The London Chamber of Commerce and Industry does not take responsibility for the disaster recovery/crisis management advice given.

