



BUSINESS CONTINUITY MANAGEMENT



Statistics show that those small and medium-sized companies that remain closed for more than five days after a disaster will face an uphill battle to stay afloat. One source indicates that over 70% of companies that suffer a major information technology interruption are out of business within one year.

Source: Disaster Recovery Journal, Winter 1997

Driven by business mandates, regulatory requirements, enabling technologies, and the changing economics of IT infrastructure, management's tolerance for operational downtime has been in steady decline for some years.

Source: The CPM Group (CPM) and Deloitte & Touche LLP (Deloitte & Touche) 2005 Business Continuity Survey.

Your challenges:

- Ensuring your Business Continuity Plans are up to date and periodically tested
- Demonstrating how they improve business resilience and increase the possibility of a quick recovery
- Making sure the content is wide enough in scope.

Our key capabilities:

- Facilitation of the Business Continuity Planning process by offering:
 - Initial training and briefing sessions
 - Workshop training
 - Threat analyses
 - Risk assessment workshops
 - Development of BCP
 - Provision of pro forma's and templates for BCP
 - Review of existing plans
 - Advice on sustainability and ways to improve.

Tips to minimise risk:

- Ensure IT is backed up and carry out the following basic steps:
 - Keep a record of your internet service provider (ISP), tel no, dial-up no, username and password
 - Keep a record of your email service provider – check if username and password are different from above
 - Create a back-up CD/DVD of all your key contacts: your employees, customers, suppliers, advisors, and personal contacts - update this data once a month, and check that your computer can read the CD/DVD
 - Ensure someone is responsible for keeping the CD/DVD safely OFF-SITE and that it is accessible at all times, including during holidays and sickness.

A robust back-up regime, together with protection against computer viruses, is a critical part of safeguarding your business.

Case studies:

Whilst undertaking a client review we discovered that there was a very heavy reliance (in excess of £30 million turnover) on a single manufacturing machine. The business also had significant combustible building construction issues and inadequate fire protection. The feedback we gave resulted in the client duplicating both machine and premises, reviewing construction materials and installing sprinkler protection.

During a Disaster Recovery Test for an IT Warm Start site, it was discovered that Tape Drive hardware was not compatible and back-up data could not be loaded. Whilst the test failed in theory, it ensured that the error was not repeated and that suitable tape drive hardware was available for the future.

During a Business Impact Analysis, it was established that critical data could not be recovered within required timescales and as a result the client has now invested in a mirrored IT site.



Chubb refers to the insurers of the Chubb Group of Insurance Companies: Federal Insurance Company, Vigilant Insurance Company, Great Northern Insurance Company, Pacific Indemnity Company, Northwestern Pacific Indemnity Company, Texas Pacific Indemnity Company, Executive Risk Indemnity, Inc., Executive Risk Specialty Insurance Company, Quadrant Indemnity Company, Chubb Custom Insurance Company, Chubb Indemnity Insurance Company, Chubb Insurance Company of New Jersey, Chubb National Insurance Company, Chubb Lloyds Insurance Company of Texas. Not all insurers do business in all jurisdictions.

This literature is descriptive only. Actual coverage is subject to the language of the policies as issued.
Form 61-01-0005 (Rev. 3/05)