



**Catherine Doherty.**  
Principal, Intelligence.  
Investit.

## Business Continuity Management for Hedge Fund Managers

Everyone knows that it is important to plan for disasters. The very useful site [www.londonprepared.gov.uk](http://www.londonprepared.gov.uk) fires statistics out: “80% of businesses affected by a major incident close within 18 months; 90% of businesses that lose data from a disaster are forced to shut within 2 years; 58% of UK organisations were disrupted by September 11<sup>th</sup>, and one in eight was seriously affected”.

Interviews of local businessmen following the Buncefield oil depot fire illustrated how catastrophic the knock-on effects of someone else’s disaster can be. But still many small firms, including many hedge fund managers (and, to be candid, many small consultancies) fail to prepare properly.

Investors are becoming more aware of the effect that disasters can have on businesses and questions about continuity planning are appearing in RFPs. The regulators have also recognised this and slipped an article into MiFID to “require investment firms to establish, implement and maintain an adequate business continuity policy” – and this will turn up in the new FSA handbook in January next year. Managers have to demonstrate to investors and regulators that they are able to manage investors’ money effectively, prudently, and also reliably. On a practical note, major incidents in financial centres are often followed by high market volatility, so it is even more important to continue being able to trade at these times.

Because the wide range of generic advice can range from inappropriate to bewildering, AIMA’s Sound Practices Committee decided it was time to establish a set of principles for business continuity management which were specifically designed for a small to medium-sized hedge fund management company. They wanted to issue a wake-up call to everyone whose eyes had glazed over at the mere mention of disaster recovery, and also to give some practical advice for firms to use.

The first step was to banish the term “disaster recovery” and replace it with “business continuity management”. The focus is on keeping the company working as effectively as possible during a period of disruption, and making sure that it returns to full operation afterwards.

Every disaster can be broken down into four key risks: loss of access to the building, loss of staff, loss of systems or loss of suppliers. However this can feel a bit abstract at first, so it can be helpful to consider particular scenarios which could disrupt the business. A hedge fund manager based in the centre of London or New York should be prepared for scenarios such as:

- A major terrorist incident which makes a large area of the city unusable for several days;
- The office building catching fire and being severely damaged by the water used to extinguish the fire;
- A local terrorist incident or health-related scare which means that nobody can get to the office for a few days - the emergency services often get the stripy tape out and create massive no-go zones while they coordinate their first response;
- Substantial travel-related problems which keep many key employees away from the office;
- A power cut lasting several hours;
- Burglary of all the computer equipment in the office, including laptops and servers;
- Computer virus corruption of key spreadsheets.

Energised by this collection of potential newspaper headlines, the planning can start.

The first stage is to identify the business critical activities across the whole organisation, how quickly they must be recovered and what would happen if they can’t be done. People right across the company should contribute to this, from directors and senior management to finance and business administration.

From this the most critical tasks in a Business Continuity context can be identified. For example FX hedging may be deemed so important that plans need to be made to ensure that it can happen instantly even in the most severe disruption, whilst client reporting is important but it may be able to be delayed for a day or two.

One key parameter here will be the nature of the funds - a volatility arbitrage fund will have very different recovery timescales from a fund-of-hedge-funds.

The company's network of relationships should also be considered. Suppliers can be both part of the solution and part of the problem:

- the administrator can contact registered investors and can restore portfolio positions, but in turn what would happen if they had a disaster;
- a locally-based prime broker may be affected by the same scenario as the hedge fund company;
- service interruption from a single key market information provider might need its own specific plans;

From this information the recovery plans can be built up. One key element often forgotten is to plan for the management of the recovery process. Who should be in charge in the first few minutes? Who decides that this really is a crisis, rather than a short interruption which will soon finish? Where will those people assemble? *(What would happen if your assembly area was also inside the cordon?)*

Who will coordinate the whole recovery, the technology recovery, the premises recovery, and who will manage communications. Note that we are over halfway through this article and that was the first **and last** mention of technology – emphasising again that this is not an IT project. *(What would happen if your disaster recovery site has sold space to many businesses in Dover Street?)*

Plans must allow for two key people to be taken out of action at the same time *(What would happen if one of them is the systems administrator?)*

Arrangements need not be extreme. It is entirely allowable to plan to move into a home office, as long as everyone can get there. Communications to staff and clients are a key part of the arrangements, but these can be done via a passworded page on the firm's website. *(What would happen if the mobile phone networks were switched off, as happened on the 7<sup>th</sup> July?)*

With the initial crisis past and the firm operating in recovery mode, it is vital to manage the return to business as usual. Some staff will need to keep going with business as usual while others switch to reconstructing the trade history, updating client files with records of conversations not made on recorded lines, redocumenting investment decisions and getting the systems back in line so that the emergency spreadsheets can be switched off.

Finally the importance of testing and updating the plan cannot be overemphasised. There is no point in having a plan that has not been tested, and just doing a desk walk-through can be extremely helpful. Plans often prove to have unsuspected flaws – one reviewer of the AIMA document said “in the test my team's desks show on the plan at the DR site were actually in the middle of a corridor”. The testing frequency will depend on the nature of the company's business, and full tests can involve just part of the staff and can be done at weekends.

Four different review and update cycles are needed – constant updating of ad-hoc minor changes such as new passwords, a general review every 12-18 months, a full reconsideration of the plans if there is a major business change such as the launch of a new investment strategy, and an extension of the plans when a new risk is identified, avian flu being a recent example.

The AIMA document finishes with a set of checklists. First there are 23 questions for inclusion in RFPs. Potential investors will be using these, they are simple and realistic questions but they do require planning to be able to give good answers.

The second checklist shows what should be in a disaster information file. This becomes a potent document as it contains all the logons, passwords and spare hardware “keys” and it could also become a major security threat if it is not looked after carefully.

The document ends with some cautionary tales. Evacuation routes which go over several rooftops but staff who suffer from vertigo. The scene on September 11<sup>th</sup> on the front steps of a prominent cathedral in New York where a huge number of firms had all decided that it was the ideal emergency rendezvous. Vital cross-linked spreadsheets which stopped working when they were restored to a different drive letter. Internet site

passwords which had been stored as cookies and since forgotten. And arriving at the assembly point and finding that nobody had remembered to bring the DR file.

The Sound Practices committee hopes that this document will prove to be a little more engaging, readable and above all useful than previous information on this topic which is now in your bin. Happy planning!

## About the author

*Catherine Doherty heads up the Intelligence services at Investit, and specialises in helping fund managers to use technology effectively.*

*She has spent the last two years developing and launching the Intelligence service, which takes a COO's-eye view of the problems behind the scenes in investment management companies. She has worked on the Derivatives, Hedge Fund and Outsourcing Performance papers, as well as giving overall editorial control to the service. Between the papers she has worked on specialist system selections in areas such as Private Equity, hedge funds and CDOs, and has continued to work in her core areas of systems strategy and planning. She has also worked on hedge fund administrator selections.*

*Catherine has worked in investment management IT for over 17 years. Prior to joining Investit she was Head of Investment Systems at Gartmore. Her previous employers include GAM and BZW, including various projects with BZW Investment Management.*

Contact Catherine Doherty on +44 (0)207 920 9000.