Immediate Action

This paper identifies the "immediate actions" carried out by a Business Continuity Manager, working within the Financial Sector in London, in response to the shocking events of September 11th 2001. It tracks the additional considerations for inclusion within their Contingency Plans, through to the identification of a "simple" solution!

The shocking events of September 11th highlighted to the World that however low the probability of a catastrophic incident, when it does occur, the scale of the impact upon an organisation and its people can be personally and materially significant.

At that time I found myself trying to come to terms with what had happened in the USA, whilst at the same time carrying out a "what-if" exercise against the performance of my Business Contingency Plans under similar circumstances:

- What-if a similar event happened in this Country, would they suffice?
- What-if key members of staff were impacted, what were the options?
- What-if our critical suppliers were affected by such a Disaster, could they continue to manage our supply chain?
- What-if our disaster recovery service suppliers had to manage multiple invocations, could they deliver our Business Recovery Plan?
- What-if we couldn't gain access to our specified disaster recovery site, could the plan work at another site?
- What-if we couldn't get staff into the City Centre, would it be possible to re-establish the communications network at another site?
- What-if we had to recover to a site outside of the City Centre, again would it be possible to re-establish the communications network at another site?

What was different now was that my "scope" had evolved to incorporate the words "multiple invocations and relocation outside of the City Centre". And, Senior Management now realised that there was a requirement to make the organisation more resilient within a single robust business recovery plan, a plan that was flexible whilst being able to manage all of the "what-if" scenarios.

So, "what-if" we could manage all of the "what-ifs", keep it simple and deliver this single robust plan that also incorporated resilience and flexibility, whilst having longer life than a Y2K Plan, what would be necessary?

Well, I obviously needed a flexible Plan, for the people & technology, which would enable the organisation to relocate to more than one secondary site, each one dependant on my "what-if" scenarios (single & multiple invocations and denial of access to outside of the City Centre). And, at the same time I would also have to "orchestrate" our staff whilst remaining resilient to our customers and stakeholders. Oh, and limit the impact on the organisations brand, image and reputation.

No problem! Where do I concentrate my activities, remember the threat is immediate and at its highest level of status. Well what is the common denominator? Obvious, my main objective should be to create a resilient communication infrastructure (voice/data/text & video), that would be able to manage the day-to-day communications delivery through to delivery Day 1/Week 1 services for a disaster (internal & external networks and technology).

Well, next question what other critical factors must I consider to make a complex plan work?

- Simplicity (always difficult);
- People (specific locations needed for each scenario);
- Communications (easy but could be rather expensive, dependant on capacity and bandwidth);
- Networks and technology (extremely complex and probably expensive, being difficult to manage ongoing changes).

Stop! Think:

- What future projects are currently being planned, for networks and technology, which could assist in delivering my solution?
- What people, networks & technology contingency options do I already hold in my “tool bag”, and;
- Will this Plan be sufficiently flexible to deliver my robust resilient solution?
- Also, have I assessed all the additional resources, either in-house or from my suppliers that can be provided contractually and yet are flexible enough to be delivered within my business recovery time-scale?
- And, by the way, what is the recovery time-scale? Has it changed so much for each scenario?

Time to consider:

- What additional technology assets do I now need to protect (Day-to-day)?
- What other elements do I need to have for “disaster” recovery (Day 1/Week 1)?
- What strategic direction must be included to manage future scope creep (larger “tool bag”)?
- What else would be nice to have (additional resources)?
- What can I live without (difficult)?

Stop! Do I have all the information? Probably not:

- What is the status of any spare accommodation currently available in-house?
- How could I ensure that the internal accommodation is “reserved” for contingency uses?
- What additional disaster recovery sites and services are contractually available from my existing disaster recovery supplier?

- What network connectivity is provided within, and exists between, disaster recovery sites managed by the supplier?
- How resilient are the processes & procedures, under normal day-to-day operations, to resource/replace/re-configure our network?
- What changes, if any, are there to the number of people and amount of services required for Day 1/Week1, following declaration of a disaster?
- How much network bandwidth and infrastructure currently exists at my secondary site(s) to manage any revision of the Business Recovery Plan for additional Day 1/Week 1 services?

And, in the event of an emergency, assuming "multiple invocations & relocation outside of the City Centre", what other factors should I consider?

- What additional contingency planning options could be made available from our disaster service provider?
- What new contractual considerations now need to be considered, with the disaster service provider, for such circumstances?

Time to daydream and recap on what would be required to deliver my objectives. Well, in the "ideal world" a range of communications terms, such as "resilient networks, 100% availability, self-healing rings", supposedly already exist. However, within the telecommunications liberalised environment where could I obtain such a solution dedicated to disaster recovery, yet capable of providing day-to-day connectivity for our operational communications & networks?

Maybe, the answer lays in establishing a "point of presence" on a shared (contractually) disaster recovery network outside of the City Centre at a point where the risk was reduced and we were able to physically access should there be a denial situation. This would require a fibre optic "disaster" ring, providing bandwidth & capacity, capable of delivering connectivity to all of my key buildings (day-to-day and disaster site(s)).

Quite a tall order, however to make it simple I concluded my solution must rely upon using third party disaster recovery resources managing a single network media that was able to integrate today's complex business communications & network technology environment? Okay, who?

Fortunately the answer was with our existing disaster recovery supplier, having just established its own "DR" fibre network between their City Centre recovery sites, with a "connectivity" point of presence outside of the City Centre.

"Eureka", with this in place we would have our own "Metropolitan Area Network" providing access to our specific contracted disaster recovery resources via the disaster recovery suppliers network. This meant that I would be able to access my "disaster" (Day 1/Week 1) critical network services (internal and external) and would be able to make my day-to-day network services more resilient, this would truly be my flexible resilient solution.

There are a multitude of questions begging an answer within the above article. However, I made the decision to concentrate on the key decision points rather than the multitude of subsequent investigations that took place. I am happy to say that today with this solution in place the organisation now has the capability to manage individual outages of critical services, whilst at the same time have the capability to relocate to a range of disaster recovery sites, dependent on the scale of disaster.

Finally, how much did it cost? Well, the easiest calculation that I can put forward is that the total annual cost, including use of third party disaster recovery site(s) and resilient services, was calculated to be less than the loss of one hours trading!

Author: Steve Yates FBCI, FICPEM, MEPS