

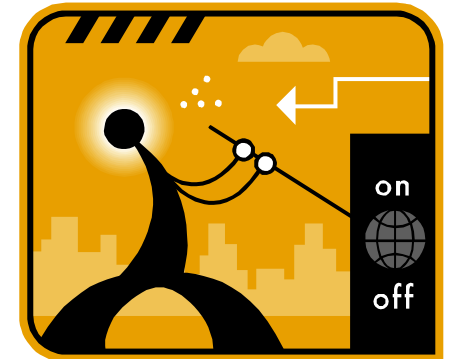
# When Disaster Recovery is Too Late

Clive Longbottom,  
Service Director, Quocirca Ltd

- Spending time carrying out commercial business?

– Or

- Spending time recovering from a disaster?



- Is it:
  - When your IT infrastructure fails?
  - When an individual loses the capability to access information?
  - When information is corrupted?
  - When information is lost?
  - When a rogue employee/external hacker carries out an action?
  
- Any or all of the above?



- Disaster Recovery (DR) aims to:
  - Provide a working environment enabling a business to re-start operations after a disaster
  - Minimise losses
  - Enable full operations to be reconstructed over a period of time
  - But – while you're carrying out your DR plan, the business is going towards being bust



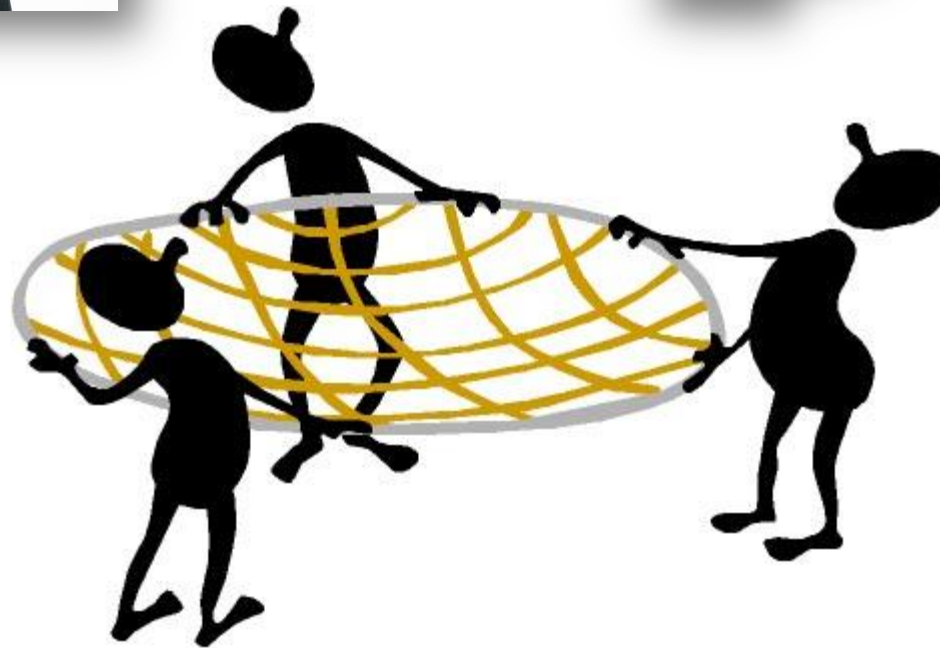
- Every second that a business is not capable of carrying out business is bad news
  - “Minimising losses” may still put you out of business
  - Any down time may drive customers away from you
    - Recovering customers can be very costly
    - The “4 second click”
  - Ensuring that a known position is worked from is difficult
    - Transactions caught in the disaster
  - Ensuring that recovered and working data are synchronised successfully is not easy
  - Plus – not all back up and restore systems work

- Of course it is
  - Things do go wrong
  - A well thought through DR plan will minimise downtime, and may save the company
- But
  - DR has to be tested
    - An IT DR plan is not a business DR plan
    - The plan (or parts of it) has to be run through on a regular basis
    - Everyone has to know their place – and this includes the general employees, not just the techies

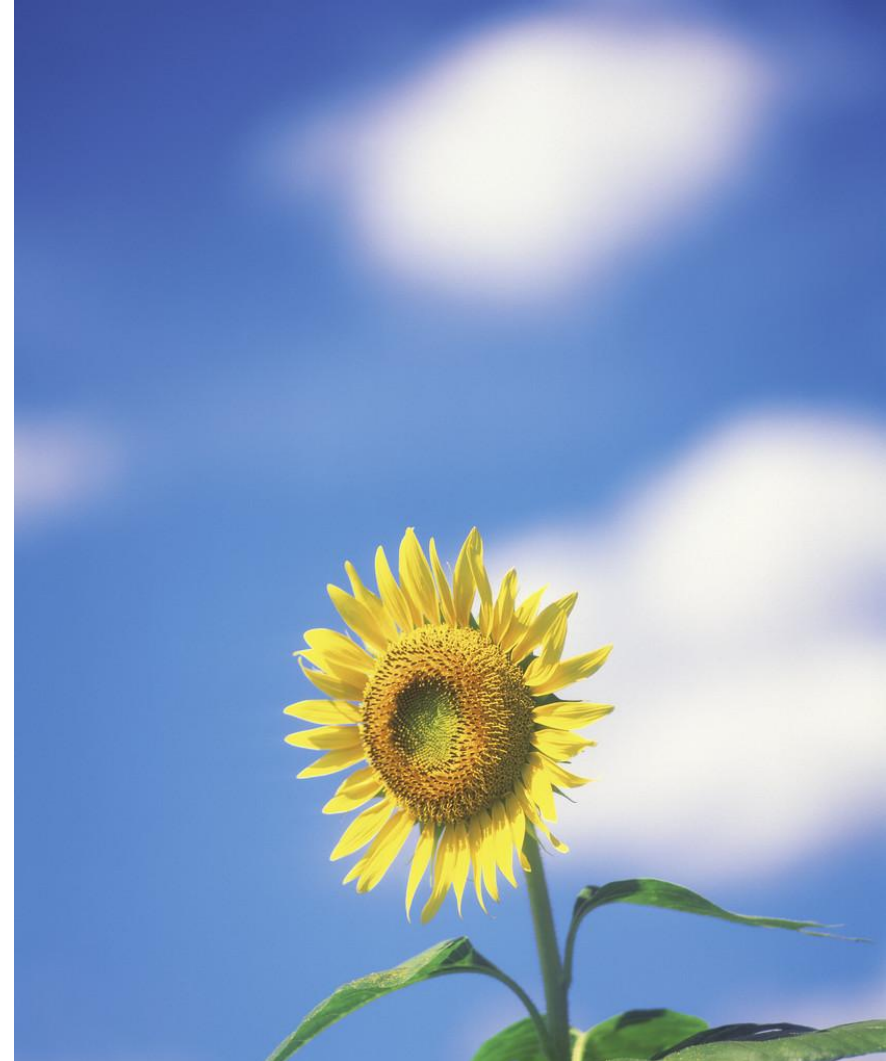


- Business Continuity aims to
  - Ensure that business operations continue through a disaster
  - Ensure that commercial activities continue
  - Provide the capabilities for issues to be resolved in a working environment with the minimum impact
- Impacts will occur – it's knowing what that impact is, what it means and managing the risks that are key





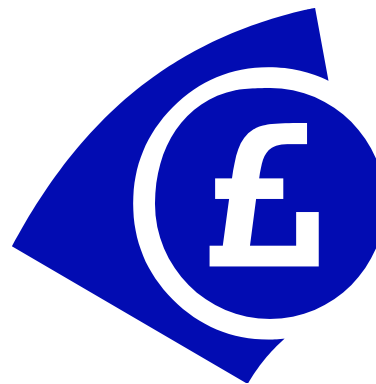
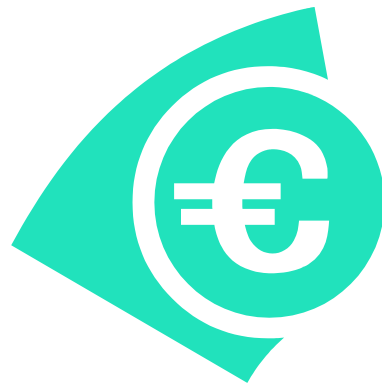
- Need the vision to think of what could go wrong
  - Needs to evaluate all possible scenarios
  - Must be able to provide details of requirements to survive these scenarios
  - Must be able to cost these out
- 
- Must NOT see any details of the DR plan



- Must be able to think beyond continuity
- Must look at the cost of survivability
- Must see everything that the BC team does
- Must identify where the BC plans may not work
- Must also cost the survivability of scenarios without the BC team's plans



- Bring together the BC and DR findings
- Evaluate the risk to the business
  - Direct financial costs
  - Indirect brand/profile costs
  - Compare cost of DR, cost of BC, cost of doing nothing
- Decide the correct path to take



Cost of BC – Cost to business of downtime < Cost of DR Then do BC  
(But have DR capability as back up)

Cost of BC – Cost to business of downtime > Cost of DR Then do DR

Exception:

Lower of (Cost of BC/Cost of DR) > Cost to business of downtime Then something wrong!



# Quocirca's Patent Pending All Comer's Guide to How to Survive Whatever the World Throws at You

1. Component failure
2. Assembly failure
3. Room failure
4. Building failure
5. Site failure
6. City failure
7. Regional failure
8. Country failure
9. Geography failure
10. World failure

1. Component failure

2. Assembly failure

3. Room failure

4. Building failure

5. Site failure

6. City failure

7. Regional failure

8. Country failure

9. Geography failure

10. World failure

- N+1 components within an assembly
  - Failover components
  - RAID storage
  - Multiple power supplies
  - Multiple NICs

1. Component failure
- 2. Assembly failure**
3. Room failure
4. Building failure
5. Site failure
6. City failure
7. Regional failure
8. Country failure
9. Geography failure
10. World failure

- **N+1 assemblies**
  - Server Clustering
  - Storage Mirroring
  - Multiple networks

1. Component failure
  2. Assembly failure
  - 3. Room failure**
  4. Building failure
  5. Site failure
  6. City failure
  7. Regional failure
  8. Country failure
  9. Geography failure
  10. World failure
- **Dual data centres in building**
    - Hot mirroring of server stacks
    - Hot shadowing of data

1. Component failure
  2. Assembly failure
  3. Room failure
  - 4. Building failure**
  5. Site failure
  6. City failure
  7. Regional failure
  8. Country failure
  9. Geography failure
  10. World failure
- Distance mirroring on campus
    - Hot mirroring of server stacks
    - Hot shadowing of data

1. Component failure
  2. Assembly failure
  3. Room failure
  4. Building failure
  - 5. Site failure**
  6. City failure
  7. Regional failure
  8. Country failure
  9. Geography failure
  10. World failure
- **Multi-data centres across same city**
    - Hot mirroring of server stacks
    - Staged hot shadowing of data (for transactional fidelity purposes)

1. Component failure
  2. Assembly failure
  3. Room failure
  4. Building failure
  5. Site failure
  - 6. City failure**
  7. Regional failure
  8. Country failure
  9. Geography failure
  10. World failure
- **Multi-city data centres**
    - Hot mirroring of server stacks
    - Staged hot shadowing of data

1. Component failure
  2. Assembly failure
  3. Room failure
  4. Building failure
  5. Site failure
  6. City failure
  - 7. Regional failure**
  8. Country failure
  9. Geography failure
  10. World failure
- Long distance multi-data centre mirroring
    - Warm/Hot server stack mirroring
    - Staged data shadowing

1. Component failure
  2. Assembly failure
  3. Room failure
  4. Building failure
  5. Site failure
  6. City failure
  7. Regional failure
  - 8. Country failure**
  9. Geography failure
  10. World failure
- Multi-country data centre mirroring
    - Warm server stack mirroring
    - Staged data shadowing

1. Component failure
2. Assembly failure
3. Room failure
4. Building failure
5. Site failure
6. City failure
7. Regional failure
8. Country failure
- 9. Geography failure**
10. World failure

- Multi-continent data centre mirroring
  - Warm server stack mirroring
  - Staged data shadowing

1. Component failure
2. Assembly failure
3. Room failure
4. Building failure
5. Site failure
6. City failure
7. Regional failure
8. Country failure
9. Geography failure
- 10. World failure**

- Maser beams
  - Coherent radio stream sent in a known direction
  - Recovery may be a problem...

- Line of Business awareness and buy in
- Cost
- Security
- Testing



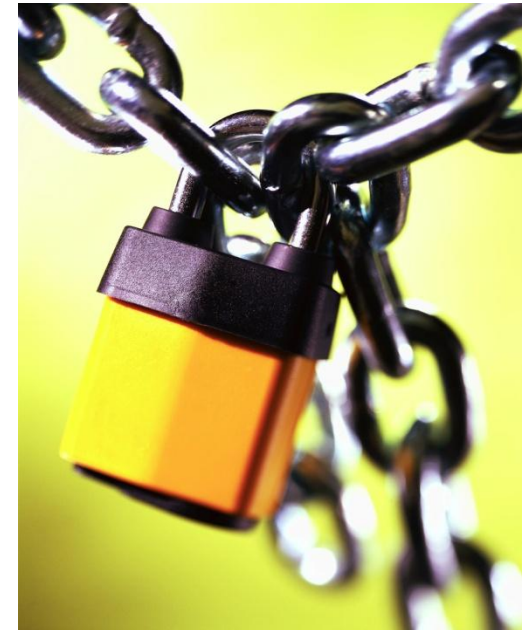


- It's their business as well
  - Are they aware of the current risks?
  - Can the business afford not to have a solid BC/DR plan?
  - It has to be a full Business BC/DR plan, anyway

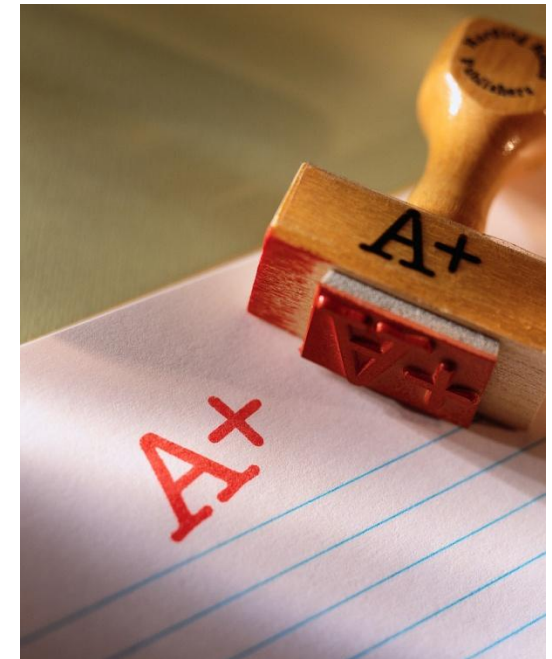
- Get a story together!
- Who would get hit most?
  - Find a C level person who can put a financial case
    - Shareholder value
- Total Value Proposition
  - Risk Cost, Value
  - Cost of not doing
  - Simplified RoI/TCO



- BC/DR involves a lot of information at rest and on the move
  - Encrypt
  - Use secure tokens (soft and hard)
  - Biometrics
  - Hardware-based tape security



- Synthetic testing
  - Any physical aspect can be tested outside of a real disaster
- Any warm/hot stand by area can be tested
  - But be aware that if a real disaster happens while under test, the disaster plan must be able to take over
- Check data integrity relentlessly
- Ensure that people know what is expected of them



- A coherent BC/DR strategy is required
- It is far better to maintain a level of capability
  - This enables a more considered DR approach to be taken
- Two teams are required – one as a air-locked team
  - BC has to be an absolute approach
  - DR has to identify where the cracks are likely to be
- The key is to provide sufficient information to the business to enable full risk management to be undertaken
  - The end result should be a blended BC/DR plan
  - Balanced by business priorities and cost