eries. But, as in any industry, there may be unscrupulous suppliers. It is the responsibility of the BC manager to ensure that he or she entrusts the survival of their company only to those vendors who apply the highest standards. The arrangements need to be backed up by a stringent contract, clearly defining service specifications, technical requirements, and SLAs.

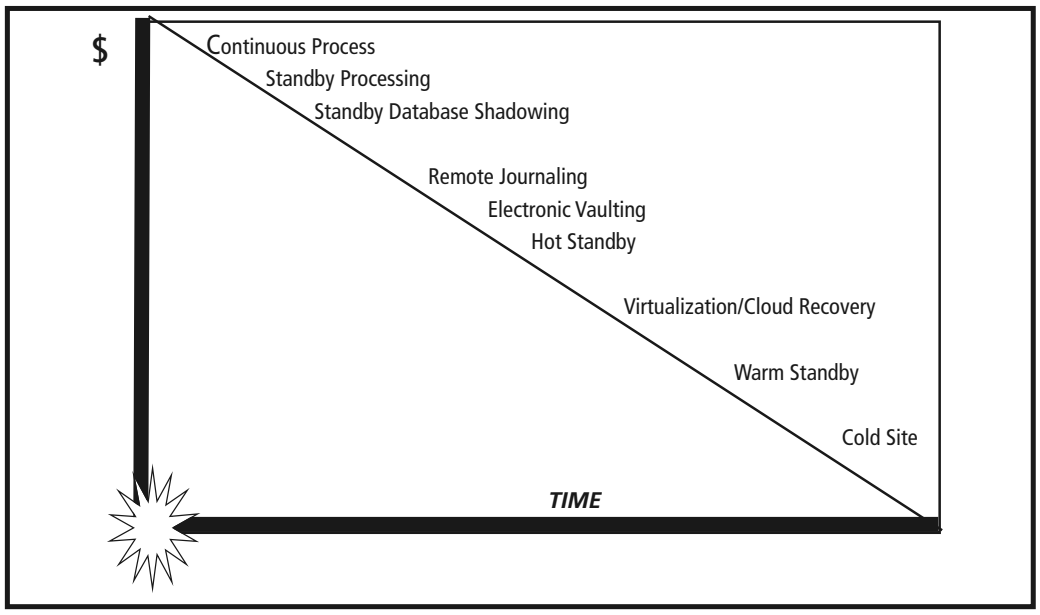

Figure 7-2. Recovery Options and Recovery Timescale

Real Life Issues

- A company had contracted for a mobile recovery solution (a standby computer room in an air-sprung trailer) that could be parked outside its offices and connected to its network in the event of hardware failure or a disaster that did not prevent the use of the whole building. When the service was invoked, the trailer was too high to go under the archway that led to the back of the building. They parked it on the road. The police ordered them to move it, since it was causing an obstruction to traffic.
- The vendor provided a quick-build building for use in the event of a disaster. Wanting to test its capability, the vendor arranged for any of its clients to call within a two-week period. The customer who invoked this test was an auto manufacturer who had contracted for it to be erected in its parking area. When the vendor arrived, a charity play bus was parked in the middle of the parking area, and nobody knew who was responsible for it. It took several hours to get the bus moved. Had this been a real disaster, those hours could have been the difference between success and failure.

7.9 Lateral and Creative Thinking

There is one more key element to devising an effective BC strategy: imagination.

It is all too easy to subscribe to standby facilities and assume replication of the existing infrastructure and business processes is the inevitable solution to a disaster. Imagination may provide alternative and more creative options. For more about working in groups to arrive at new solutions, see Appendix D in this book.

By all means consider the obvious – but let's exercise imagination, too.

Real Life Issues

- Several organizations had a process whereby trading between them was periodically accounted for and settled. Reviewing the actual settlements, it was clear that although significant sums of money were involved, the fluctuation was usually in a relatively narrow band – less than 5% – and the level of discrepancies was low. Since each organization kept records, the settlement position could be based on this in the short term and would buy a month in which to recover, substantially reducing the cost of disaster recovery.
- A fashion house manufactured and supplied garments to retail outlets. When it lost its production facility and computer installation, it survived by buying products from its competitors, having them relabeled and delived directly to its own retail outlets.
- Senior personnel from internal audit, human resources, and other support departments would be drafted into customer care during an emergency to handle customer issues proactively and staff help-line numbers.
- A cash-handling operation normally done in-house would be contracted out to a security company in a disaster.
- An organization had critical deadlines: they had to meet a tight deadline to provide input to the contractor who added a finishing process to the product so that the output could meet an immutable deadline. The solution was to find a contractor who could do the job quicker.
- A payroll operation would be replaced by an emergency payment (calculated each payroll and based on average earnings, supported by a payroll help-line making additional payments for special cases). Handling payroll in this way would release sufficient capacity to enable mission-critical computer applications to be run at another site.
- Internal audit used notebook PCs, most of which would be re-allocated to key staff in an emergency. Key staff would recall offsite backup disks of work in progress, and they and their team would handle critical work from home for the first week following the disaster.
- Although one company had a manufacturing plant, when it reviewed its BIA, it realized its vulnerability was in production and its strength was in marketing. It closed the plant and stopped doing its own manufacturing.

7.10 The Role of Insurance

One recent survey claimed that insurance actually paid out only $1 in every $50 loss. This seems low, but it is certainly our experience that insurance rarely covers more than 40% of the real loss.

It is vital that the BC professional understands the role of insurance in BC strategy, particulary its benefits and pitfalls. Insurance rarely covers the full cost of disaster. One recent survey claimed that insurance actually paid out only $1 in every $50 loss. This seems low, but it is certainly our experience that insurance rarely covers more than 40% of the real loss. For example the major meteorological phenomenon El Niño in the 1990s was responsible for 80 individual catastrophes generating total losses estimated at $18 billion, while insurance is alleged to have covered just $2 billion of this. Moreover, insurance looks at profit forensically: that is, loss of profits is likely to be assessed on profits immediately before the disaster or during the same period in the previous year.

Insurers have a duty to shareholders to return dividends. So insurers are generally getting more selective about accepting claims as valid and, when accepting valid claims, about how much will be paid out. Increasingly, negligence on the part of the insured may lead to a reduced payout, and the interpretation of negligence is open to debate. For instance, does failure to have a BCP (to limit loss) constitute negligence? Indeed, recent conferences in London are designed to help insurers interpret clauses in order to legitimately avoid paying out on claims.

All too often, the BC manager or the line manager does not know what insurance is in force – they just assume the corporate insurance manager or risk manager has it covered.

Unfortunately, insurance brokers do not always understand the detail of the business they are insuring (especially high tech businesses). Also, the the insurance broker may be negotiating with a finance person (who again may not fully understand the technology). The result may be an ambiguous insurance policy that misses key points and provides inadequate coverage. It is therefore important to review your insurance policies and, if in doubt, ask the insurer for an unambiguous definition or clarification. Here are just a couple of examples of ambiguous words found in insurance policies:

- "Data-carrying materials" – so disk arrays and tapes should be covered shouldn't they? But does this include copper or fiberoptic cable? Filing cabinets? Safes? PCs? Laptops? BlackBerries or other handheld devices? Or does it mean just the hard disk in PCs and laptops?
- "Computer" – with chips in virtually all equipment, do we know what a computer is anymore?
- "Maintenance must be in force" – to what level and by whom? The original equipment manufacturer (OEM)? If we have not advised the insurer of a third party maintenance contract, does this mean we have withheld "relevant information?"

Self-insurance is not necessarily a complete solution. If you are self-insured, it may mean that "corporate" has reinsured loss – or are they carrying the risk themselves? Are they carrying all of the risk, or do they have an insurance reserve? As a BC planner, do you know how to get your hands on the insurance reserve? Do you know how big the insurance reserve is? Is it enough? One way or the other, the insurance reserve has to be funded, and eventually it comes back to the bottom line.

What value do we place on the asset? Typically this may be a depreciated cost – but depreciated how? Tax depreciation or book value? Do corporate depreciation policies really reflect the true cost of acquiring similar equipment? And what if the asset is worth more to the business than its book value? Are we insured for exact replacement of an asset (like for like) or for the nearest equivalent and if for the nearest equivalent, what if it is not fully compatible (say with existing software applications or with other parts of a production process)? Who pays for redesign? Is just the equipment cost covered, or the full project cost of reinstatement to the predisaster status?

Does insurance cover continued cost of rent if the rented premises we are occupying gets destroyed?

What risks are insured? Beware the "all risks" policy – such policies usually carry exclusions and, oddly enough, do not cover "all risks." In some policies (notably cases concerning malicious damage or fraud) for an effective claim, the claimant may have to prove the identity of the perpetrator.

Loss has to be proved: inventories, asset registers, financial records, records of costs incurred in the disaster, and other evidence is essential if a claim is to be successful. We can insure for loss of profits, cost of cash flow disruption, interest, extra cost of working, and many other things. But to be sure of getting paid, the claimant has to prove the loss beyond reasonable doubt. So there need to be preagreed upon formulas with the insurers, supported by inventories and possibly videos and photographs. Insurance for cash flow disruption, loss of profits, and extra cost of working has an "indemnity period" the length of time during which such insurance will be paid, anything from six months to three years. It is important that the indemnity period covers the likely duration of such losses.