



Hosted software as part of a business continuity contingency

Any business faces minor downtimes and major unknowns. It is important therefore that contingencies are built into the business processes to ensure that important information is protected in the event of a planned or unplanned closure of the business. It has once been said that any investment into a Business Continuity Program (BCP) is a waste of valuable resources. And it is true that if a strict ROI calculation is attributed to such a program it is likely that it would not provide a sufficient justification for such an investment. However, anybody who has experienced a cessation of business activity will know that not having a BCP spells disaster and in fact it is a small cost to bear in relationship to the losses the business incurs during such an event.

Our recent history is filled with events that "were unthinkable" but that actually happened and which are all reminders that a BCP should not be disregarded. It is an accepted fact that following a major fire almost half of businesses fail to reopen and then close to a third of those that do reopen do not survive beyond three years. Those are everyday examples and the list could easily go on and on building up an unassailable argument for a BCP.

There are also smaller scale events where because of the temporary nature of the business interruption there is no life threatening effect on the business but the amount of time spent recovering lost information can be seriously distracting and in many instances where the information is permanently lost it can lead to severe problems for the people or organisations affected by such a loss. All distractions however small create a cost to the business as they take away resources from normal business activities and lead to increased overtime, more defects (which have to be fixed at a cost) or simply greater stress which means lower staff efficiency.

A BCP is ultimately a simple methodology for identifying areas of risk, creating contingencies, assigning responsibilities, communicating its benefits to the organisation and then following up with regular audits and live tests. But as in any aspect of a business's activities it needs the commitment of senior management and staff for its processes and disciplines to be effectively imbedded into the organisation.

While, this article does not go into the subject of how to construct a BCP, it does, as the title suggests, describe how a hosted software product can be used by an organisation as part of its business continuity contingency.

The definition of a hosted arrangement is one that is held as a guest by a third party. This means that the third party not only holds the hardware and software on behalf of the client but also takes care of maintaining both the hardware and software as well. In the specific case of a hosted software the

product is owned, hosted and managed by the organisation that developed it and is then rented out from its hosted location for specific periods of time to a number of different companies. The hosting location is always remote from the business locations of the clients and the software product is accessible over an Internet connection. This provides a dual benefit of operating from a remote location that is protected from any event that could happen to a client's business location while at the same time being able to be accessed from any PC and from any location, whether primary or alternative, with an Internet connection.

An example of a specific instance would be helpful at this stage. Company A operates from a single location with its offices, manufacturing and distribution in the same building. A small fire in the plant sets off the sprinkler system in the entire site and the fire's spread is restricted and quickly put out. The damage is limited to the factory and it is quickly cleaned and is up and running again within a couple of hours. However, the damage from the sprinklers in the offices is substantial and all electronic equipment is permanently damaged and the storage disks are corrupted and it is not certain that anything can be recovered from them. However, the company used a hosted software to run its quality systems and its customer management with the data being held at the hosting location. So with the help of a new PC, an existing live broadband connection and a new printer, Company A was able to access its account and retrieve its orders, print out its latest production procedures from its quality system and have the factory starting production on outstanding customer orders as soon as it had been cleaned up from the fire. There obviously could have been some mitigating measures that should have been installed prior to the incident such as different sprinkler systems in the offices and the factory and a gas based extinguisher for the electronic equipment but the management was not willing to accept the extra expense at the time.

As an observation Company A was able to reduce its downtime because it had systems and procedures in place to enable it to recover key information far quicker than had it disregarded such contingencies and taken the attitude that "it would never happen to us". Clearly, the hosted software product at a remote location with its standard and premium back-up models combined with its Internet connectivity had an important role to play in Company A's business interruption contingencies.

But let us not forget that a hosted application also provides a cost effective alternative to a standard client server application while at the same time having the structure for protecting against the unexpected.

Written by Christopher Stainow of Lennox Hill Ltd on 4th December 2006