

Extract from Jim Lee's 'midrange matters' column in iSeries365 and iSeries News UK

## **COLUMN: Midrange Matters with Jim Lee: HIGHLY AVAILABLE...BUT USEABLE?**

*Could a hosted HA solution be the answer to your business continuity plans?*

If you stand and look at a server, you can begin to create the checklist of things that will go wrong and affect its availability. The list, initially at least, will involve hardware failure. You might build in resilience with a RAID disk array and dual power supplies; more esoteric is the opportunity for virtualisation of the environment with clustered processors.

Next, software comes into the equation. Operating systems failure, middleware failure, applications errors -- each with its own attributes for being hacked, for failing, for error and recovery. Solutionising becomes more difficult. You might replicate the data but switching the services is not so easy. It is certainly not a given that users will experience uninterrupted service in terms of applications.

If you combine the hardware and software possibilities for failure, the combinations and permutations display truly frightening complexity. Maybe, just maybe, you envisage a proposal for dual everything with replication.

Turn around from your server view and you begin to take into account the infrastructure factors. Power, communications, fire, heat and RF interference are prime possibilities for causing failure. Tick off solutions -- uninterrupted power supplies, no single point of failure in switch links, diverse routing for communications, gas suppression for fire, RF isolation...

Stop! You are addressing symptoms, not problems. Let us begin again, this time defining the problems.



# Midrange Matters

[www.campbell-lee.co.uk](http://www.campbell-lee.co.uk)

How long can your company exist without the services and information provided by each server? Expect a different answer, for each application's service, for each server. Some companies can survive without the back office server for days but the same company may not be able to survive without email or telephones for even an hour. Create a list of functions and related urgency. Then translate this to servers and software. This provides a definition of the problem to which a solution for resilience and recovery must be found.

Communications resilience requirements follow exactly the same analyses. What communications are truly critical? Voice, fax, email all have an equal call over inter-office data links and pipes to the web. Few companies can afford diverse routing with duplication of high-speed links. It may be possible, however, to arrange failover to a simpler but slower link that has an alternate route served by a different point of presence of your telecoms provider. This may suffice for emergencies and is a great deal more economic than diverse routing with alternate fibre.

Basically, high availability is, like most things in IT, about service to users and hence to the business. Too often, things are done in the name of technology. Justifications are provided on a fear, uncertainty and doubt basis. Threats to infrastructure itself are listed. Doomsday scenarios are weighed against budgeted spend for solutions. But the actual effect on the business is given a lower weighting than the probability factors of the scenario. This is wrong.

Let me give you two actual experiences that illustrate this. The first was a real business continuity invocation. Fire had destroyed or damaged servers and desktops. The customer's staff transferred smoothly to desks with desktop computing attached to rebuilt servers, all as planned.

The business of the customer involved hundreds of faxes per day. Without the ability to send/receive faxes to/from its customers the business was effectively dead. The issue was resolved relatively quickly which was great good fortune (and I have to compliment BT since they are so often slated and rarely praised).

What this underlines is that the very high-tech aspects of replication and rebuild had been planned and commissioned but a business fundamental had been overlooked because it was relatively low-tech. Plans had been based on technology before business.

Next, another fire story. As a result of a fire in an adjacent building, a company was refused entry to its premises. Hasty arrangements were made to site key staff in a serviced office. Surprisingly, contact was successfully made with the company's servers by remote access. Jubilation -- no server rebuild from backup was required. Business continued for days.

The subsequent demolition of the adjacent building took out communications. For almost a week, the company's servers ran happily in splendid isolation as the business ground to a halt. Because of the period during which business continued by remote access, the plan that provided for server rebuild could not be implemented. No back-up was available that reflected three days business.

The lesson here is that, when you have a plan, stick with it. Adapting the tactics because of technology can defeat the strategy. The strategy in this case was based on rebuild from backup and re-routing communications. When communications initially survived nobody re-evaluated the effect on the business and the new risks.

High availability is a huge driver for outsourcing. The analysts frequently compare and contrast whether outsourcing is more or less expensive than in-house IT, whether cost control can be delivered and whether service level contracts can be relied upon when prepared by the uninitiated. All well and good: bring high availability into the equation and the whole subject of outsourcing is on a completely different



footing.

Larger enterprises with high dependency on server services have long since positioned replica servers in distributed data centres with resilient communications connectivity. Smaller or emerging companies are unlikely to afford such investment. Two clear requirements will stall the board of such companies -- duplicate servers and communications. This is big bucks for little immediately obvious value-add.

When the requirement for high availability has been properly researched and it has been business-driven, guess what? Remote hosting of critical servers proves a viable option. After all, you are going to need the communications capability for remote replication. Why not simply move the primary server to a secure and resilient centre? It won't lose power or set on fire. Communications links at a data centre are likely to be resilient and diverse. Security in almost every dimension is likely to be stronger than can be achieved in-house.

This form of hosting is nothing like the notional concept of outsourcing. The in-house IT team is still managing IT services. It is still managing the applications. It is still servicing the business. The only devolved responsibilities may be server environment management and media handling. Nor is this a slippery slope by which the hoster eventually assumes total outsourced control of a company's IT. We have many such hosting relationships with customers. The focus is high availability. The service is high availability provisioning. The dreaded outsourcing word is never used.

One last thought. High availability is about making computers ultimately available for people to use. A business continuity plan is perhaps even more important than a high availability strategy. What is the point of having computers that are available if the people who need them are in disarray?

***Jim Lee is Managing Director of Campbell Lee plc***