

AN ICM ASSURITY CASE STUDY

Web Hosting – The Hidden Dangers

Despite the importance of e-business, many companies entrust key aspects of their business to external suppliers. However, what happens when things go wrong? Bryan Hall, from Business Continuity Service providers, ICM Assurity uses a Case Study to outline the dangers and ways to avoid them

In common with a large number of organisations, Sea Containers Ltd, a market leader in its three main business areas: passenger transport, leisure and marine container leasing, chose to use the services of a third party for their web hosting.

After a rigorous selection process which demonstrated all the required due diligences, a specialist in security and firewall protection, I will call them the ISP provider, was chosen. The site that they would be hosting included Sea Containers main front end website, the data for its Marine Containers leasing division plus its Ferries Reservation system. The site was also used for general corporate data on the company, its Divisions and subsidiaries as well as Investor and media information.

To begin with, the relationship with the ISP Provider was reasonable, but a series of small scale and easily overlooked issues started to arise. Communication with the ISP Provider had never been a strong point and information on the security of the website was difficult to obtain. To start with this did not seem to be particularly problematic, but as the lack of information continued some real concerns began to arise not least being the fact that without the security data, how could the server, and the site, be replicated?

Suddenly the service went from bad to worse: requests for small changes to the site went unanswered, or took an excessively long time to be completed. This decline in service could easily have been overlooked, but Sea Containers were formally monitoring all contact with the ISP Provider. Then some rumours about the ISP Provider's financial position suddenly started to circulate in the marketplace and it soon became very clear that they were in trouble. So was Sea Containers website.

Given the PR and financial contribution that the website made to Sea Containers business, any interruptions in service would have serious consequences.

Over a period of a few weeks, Sea Containers were able to confirm that the ISP Provider was indeed in serious financial difficulties and that it could well cease to trade at some stage over the next few weeks. Action needed to be taken.

An engineer from the ISP Provider, who had built up a good relationship with the Technical Support Manager at Sea Containers, tried to help and the process of replicating the website was begun. It soon became a race against time, however, when it was discovered that the ISP Provider was likely to exceed its funding within seven days. Could Sea Containers even formulate a plan, let alone put it into action before the ISP Provider went down?

Sea Containers contacted the major ISPs but quickly discovered that all of them required a minimum of 30 days to set up a new service.

It was at this stage that Sea Containers thought about the Disaster Recovery Plan with ICM Assurity. Although the contract did not cover this particular requirement, the pending 'disaster' was such that it seemed logical to see whether ICM Assurity could help.

At a basic level, the existing communications connection between ICM Assurity and Sea Containers could be used to provide an uninterrupted, if fairly minimal service, but Assurity were able to come up with a much better solution.

Having witnessed many similar circumstances, ICM Assurity had in fact just launched a new Internet, Email and ISP recovery service called **e-b@k**: a product specifically developed to enable immediate recovery of mail servers, instant Internet access and temporary ISP provision.

Coincidentally, Sea Containers were in the process of looking at **e-b@k** with a view to installing it. Although not intended to be an alternative ISP service, ICM Assurity reconfigured the system so that a secondary ISP route was immediately available and also provided the necessary bandwidth and net addresses with a replacement server allocating addresses to each member of staff as they logged on. Although the process was slow, each user had to be configured individually, by working through the most critical, generally customer-facing employees first, a new system was gradually built.

The timing of the whole exercise was crucial. Despite the complexities, all the work was completed within a week, just a day before the ISP Provider finally ceased trading.

The lessons are clear. Sea Containers were very fortunate on two fronts: one, that the ISP Provider's decline in services and financial problems were noticed and acted upon; two, through an existing Disaster Recovery agreement, they were able to take action before the worst happened. The damage that would have been done if the service had just stopped when the ISP Provider ceased trading would have been a disaster on its own. It would have been compounded, however, by the fact that the cost to put things right after the event would have been considerably higher than those for preventing the disaster in the first place. This is a lesson that most other companies would do well to learn.

Sea Containers is registered in Bermuda and has regional operating offices in London, Genoa, New York City, Rio de Janeiro, Singapore and Sydney. It is listed on the New York and London stock exchanges.

In addition to its three principal divisions, the Company has associated investments in property, publishing and plantations.

Last year it had a revenue of US\$1.4 billion and some of its famous brand names are Orient Express Hotels, Great North Eastern Railway (GNER) and Hoverspeed.

ICM Assurity Ltd is 100% owned by ICM Recovery Services plc the Business Continuity Service Provider of the Year 2003.

ICM Assurity Ltd,
1-2 Prince's Court,
Wapping Lane,
London
E1W 9DA
Tel: 020 7488 3344
Web: www.icm-computer.co.uk
Email: bryan.hall@icm-computer.co.uk