

Communications & Networking, June 2003, Vol. 6 No. 6

Fusepoint chief exec shares his views on security, redundancy and intrusion detection

6/4/2003 10:21:04 AM - Robert Offley

by ITBusiness Staff

It's not enough to have a disaster recovery plan, according to Robert Offley. You have to test it every once in a while.

Offley, chief executive officer of Fusepoint Managed Services Inc., says companies that don't want to go belly up in the event of a disaster should have several different sites, and several different cables leading into those sites. Fusepoint's services include intrusion detection and disaster recovery. Offley, who joined Fusepoint last year, has worked with Internet service provider PSINet in Europe.

Offley recently talked with C&N staff about the need to test disaster recovery plans and build redundancy into the network.

C&N: What are the top security concerns for IT network managers?

RO: More and more, there are organizations that, with enough resources and effort, could bring down the Internet for a number of hours. There's been a number of events over the last few months that have caused huge impact to Canadian business. It's viruses, it's denial of service attacks and it's people trying to hack in to the data within your network.

C&N: What are some examples of human error that companies should be aware of that could affect either security, or their ability to recover data in the event of a disaster?

RO: I think core to every business is having a disaster recovery plan. A plan isn't something you leave on the shelf, bring down, blow the dust off and have a look at it when you have a disaster. You have to test your disaster recovery plan on a regular basis. We've seen scenarios where companies thought they had been backing up their data off-site. They have a disaster or impact to their business, they go to recover the data, but it hasn't been tested. We have one example of a customer who went to recover off their backup site, and there was a piece of software which was corrupting all the data, and it took them three or four weeks to recover that data. I think one of the most important things is to have it documented —people change within the business.

C&N: What are some of the networking issues that you see when it comes to data recovery?

RO: You have to provide redundancy right through the whole system. We put ourselves in a position where we have multiple providers coming in to our facilities. We have multiple geographically-diverse facilities. We also have different fibre routes into our facilities. For some of our customers, we will provide load balancing across the facility.

C&N: With respect to intrusion detection, I understand you have that capability built into your system. What sort of things should you be watching when it comes to intrusion?

RO: You need to have a team focussed on intrusion detection seven-by-24. It's not just about developing a security policy and applying it. It's something where, like any form of defence, you have to be constantly understanding who's attacking you. We can offer that service to multiple customers much more cost-effectively than a customer going out and getting their own dedicated team. I think people are realizing it's not just about making a (set of rules) and just hoping everything's fine. It's about seven-by-24 service.

C&N: Do you see any issues for companies whose primary site might be located in an area where

you don't have fibre optics, you might not even have ISDN? Do you have any perspective on the implications that that might have for disaster recovery?

RO: I think the key thing for disaster recovery is you have to look at your applications and any ones that are critical to your business. Critical could be defined as where you can't afford to have down time — financial transactions, anything which is critical to your business. If you're supplying perishable foods, your logistics becomes a critical application. Today, you have to provide an environment whereby there is full redundancy of power, networks, people and processes.

C&N: Is there any particular service that you think has really taken off in the last year or two, in terms of revenue, or just interest from the customers?

RO: It tends to be anything around security. When you look at a scenario, if it's a critical application, we find more and more people try to do load balancing, looking to have maybe two or three redundant systems and maybe host it in different locations with load balancing. We always talk about computer systems, but it's the people that are most important. People can actually come and have dedicated desks that they can work with at some of our facilities, or we can actually ship trailers on to their sites. If your main site goes down, we can provide places for people to go and work on their computers. If your application doesn't need to be always up and always secure, and can maybe be up in 24 hours or 48 hours after a disaster, we can actually ship the hardware environment to one of our locations or one of the customer's locations and restore the data on to that. In today's volatile climate, businesses cannot afford to stick their heads in the sand and hope for the best. You have to put careful thought and preparation into a plan, and build a virtual bunker, should there be any unforeseen problems.

[Print story](#)[email to a friend](#)[Back](#)[Back to Top](#)