

Protect your data

by Toby Osborne

Disaster recovery technology protects IT assets

FROM FIRES AND FLOODS to blackouts and terrorist attacks, disasters strike unexpectedly. Last year's crippling blackout, as well as the tragic events of September 11, 2001 and recent terrorism, highlight the increasing need to protect against the unpredictable.

Data is a valuable commodity that can be vulnerable to loss or damage. Which is why many in the public sector are turning to back-up and recovery specialists to protect their IT assets from the risk of disaster.

"Disaster recovery in and of itself is not really a product; it's a whole philosophy," said Craig Andrews, technical director of VERITAS Software Canada – a storage software company that offers storage management software for data protection, application availability, and disaster recovery. With a 60 percent Canadian market share, their public sector clients include VIA Rail, Teranet, Bruce Power, Ministère du Revenu du Québec, York University (Toronto), University of Guelph (Guelph, Ontario), and McGill University (Montreal).

There are "different solutions for different objectives," said VERITAS' Andrews. The most popular solutions are back-up and recovery, and data replication. For the uninitiated, 'back-up and recovery' can simply be a case of "copy the data on to a tape, slip a tape in a vault somewhere and, if you need it, get the tape out of the vault and get the data back," he said. "But, the downside of that is typically it could take two or three days to get the data back, by the time you get it out of your vault." By opting for data replication, which is "essentially real time copying of the data from your primary site to a secondary site," you could get your data in a timelier manner.

Because of the variety of recovery technology software available, the individual needs of the business or organization can often be met. "Sometimes the customers themselves know what they want and we provide products," said Andrews. "Sometimes we work with the customer to help them to find what they want, what they need." Generally, the following two com-

ponents are considered when selecting the most suitable software: the recovery point objective (RPO) and the recovery time objective (RTO). "The RPO is about how much data loss you can tolerate in your environment. RTO is about how quickly you need to get something back up and running," said Andrews.

For critical data, the majority require low data loss and a rapid recovery time. Andrews suggested data replication may be the best option, however, 'clustering' is another solution that can guarantee that systems are online as quickly as possible.

"Clustering means that an organization or department has multiple machines, multiple host systems, that can run a specific application," said Andrews. "If one system fails then another system can start running that application right away. That can be done locally, within a data centre or, you can move the whole application to another data centre elsewhere."

The ability to replicate files or move an entire application to another data centre is advantageous, not only to safeguard against disasters like a power blackout in a specific grid area, but to guarantee business continuity. "Whatever the reason that [organizations] can't access their data – systems aren't available, people aren't available, [employees] might have an illness; look at the impact of something like SARS... Organizations want to have up-to-the-second data, so that a database being updated would be replicated immediately at a secondary site somewhere else," said Andrews. "And that secondary site could, geographically, be anywhere."

"Disaster recovery really encompasses a lot more than just the technology," noted Andrews. "Normally it is broken down into two areas – business continuity: which encompasses the people, the facilities, the business practices; and then disaster recovery: which really focuses upon just the technology and making sure that the technology is up and available."

Many IT departments are aware of the importance of having a reliable recovery

process as a basic requirement. Guelph University has been a VERITAS customer for eight years, and before that "it was a standard practice in any mainframe type environment that you always had back-ups because lost files, corrupted files were a way of life," said Doug Blain, manager of IT Security at Guelph. "So, we knew we had to have the same discipline for our UNIX servers. Because, you know, you don't need a terrorist to [erase a file]; any user who puts in the wrong key strokes can accomplish the same task. You always have to have some way to recover the files and that was typically the ability to have regular back-ups, bank those back-ups, and do restores from them."

Today terrorism is undeniably a growing concern. According to a recent survey of IT managers conducted by Dynamic Markets Ltd., a third of US respondents said that terrorism first prompted them to create a disaster recovery plan. A quarter of global IT managers warned that their company could be at serious risk if they did not have their current recovery plan in place and disaster struck.

York University converted to VERITAS NetBackup software back in 1999, and Dominic Nolan, senior project manager in Computing and Network Services, said he is presently "managing disaster recovery and data storage projects to improve [York's] disaster readiness. Recent events, [for example] the East coast power outage in August 2003, have influenced our disaster recovery decisions, but at this time our focus is on events that would impact key business services provided through our main data centre," said Nolan. "Events affecting large areas beyond the campus are difficult to defend against. We send our back-up tapes off-site to protect our data from major disasters."

The 2003 blackout was financially devastating for Ontario and parts of the US, but prior to that America suffered a far worse disaster. "I would certainly say that events like '9/11' have created a higher level of sensitivity to disaster recovery," noted

VERITAS' Andrews. A sensitivity that has seen business at VERITAS increase "incrementally – but, I wouldn't say that business has doubled or anything. But, I would say that most organizations have stronger initiatives underway."

The federal government has begun improving its data protection; Statistics Canada, the Department of National Defence, and the Department of Foreign Affairs are all clients of VERITAS. "Certainly [disaster recovery is] an area that we're focussed on for the federal government market place," said Andrews. It also helps that one of the company's most notable success stories is VIA Rail, a Crown corporation.

"We switched [to VERITAS] in 1999," said Ghislain Pelletier, systems analyst for VIA Rail. "I guess 'Y2K' was a big factor – the year 2000. We weren't having reliable back-ups, and had to do something. We decided to search for a solution."

"We wanted to go to more of an enterprise-class software, and were looking for something that could do multi-platform back-ups reliably – LEGATO (Networker) and VERITAS (NetBackup). At the time, those were probably the two biggest [under consideration]." VIA requested quotes from the two companies, although Pelletier "had some experience with LEGATO already, so it was just a question of evaluating the two software, and we chose the one we thought was better," she said.

Nevertheless, even world-class storage software needs an update every now and then. "We're working on updating [NetBackup] to a new version and we are running into some difficulties," admitted Pelletier. "We've been testing it for a few weeks now. We need to move up [to version 4.5] because I'm running version 3.4 which is not supported fully anymore."

Meanwhile, York University has 'outgrown' its current technology and hasn't ruled out shopping around. "We used NetBackup for a number of years, with several back-up servers and tape libraries, but we've outgrown the capacity of our current setup. We're looking to improve that," explained Marshall Linfoot, manager of UNIX Services at York. "A project team has been working on requirements for this RFP [request for proposal] to address our back-up needs – that doesn't necessarily mean replacing VERITAS NetBackup; we're interested in moving away from tape back-up

to more of an unattended, online storage type of approach. We're trying to keep our options open."

Looking towards the future is obviously a large part of disaster recovery planning – including, the future of disaster recovery technology itself. "One trend that has certainly impacted disaster recovery is the simple growth in data," said Andrews. "Industry studies show that a typical organization will experience about a 40 or 50 percent annual data growth rate. So, a solution that may have worked a year ago

might not work today." Another trend is "the world in general is moving towards '24/7' availability. Those kinds of environments are becoming more important, so again, that has implications for data protection and data availability."

Perhaps, ultimately, with the right recovery technology the unforeseen won't necessarily be a disaster. *mm*

Toby Osborne is a freelance writer based in Gatineau, Québec.