

November 24, 2003

News for Builders of Technology Solutions

-  SUBSCRIBE TO MAGAZINE
-  SUBSCRIBE TO NEWSLETTER
-  CHANGE 'TO' ADDRESS

**MAIN:**

- Breaking News
- Advertising Information
- Press Releases
- Contact Information
- Archives
- Feedback
- About Us

o

**IN THIS ISSUE: Data Management**

Jul 12, 2003 | CRN Canada-Paul Lima



Data is everywhere. On the hard drives of servers, workstations and computers in head offices, branch locations and remote facilities. On the home computers of employees who telecommute or work evenings and weekends at home. On laptops and PDAs of mobile executives, sales representatives and field staff.

How, then, is the IT department to cope with data storage, backup and

recovery? What if servers crash, laptops are lost, or home computers are stolen? What happens to the data, some of which may be mission-critical?

These are all vital questions, and you can blame it all on distributed computing, where data is stored on computers and computing devices in a multitude of locations. With the exponential explosion in, and the critical nature of, business data, we are seeing a return to more centralized data management systems, says Tony Fernandes, vice-president of technology infrastructure with Inventure Solutions, the IT subsidiary of Vancouver City Savings Credit Union (VanCity).

VanCity is Canada's largest credit union, with \$8.2 billion in assets, 286,000 members and 39 branches throughout Greater Vancouver, the Fraser Valley and Victoria. The company has about three terabytes of data, including optical storage, to store and manage.

As with any financial institution, real-time data storage, backup and recovery are significant issues – especially when each branch has its own server that needs to be backed up daily. Late in 2002, Inventure Solutions upgraded VanCity's enterprise storage environment by installing EMC Canada CLARiiON

CX600s in its two data centers. The goal was to consolidate mission-critical banking and transactional systems as well as non-critical data from more than 100 data sources on one storage area network, Fernandes says.

After testing – and a pause for the hectic RSP season – the system was rolled out in April 2003. "We were looking for high data availability and a never-fail way of managing data," Fernandes says of the system that replaced servers at each branch with a central data storage and management system.

"Many management issues are facilitated by having all data stored in one place," he adds.

Branches no longer have to backup data locally, freeing staff to focus on customers. Now that the IT department stores and backs up all data centrally, Fernandes knows backups are done correctly. In addition, he no longer has to dispatch IT staff to deal with overloaded branch servers. It's also easier to add data storage capacity, with no down time at the branches, now that storage is centrally located.

Centralized data storage offers an additional bonus. VanCity now executes its business continuity strategy between its two CX600s, with data replication and mirroring carried out seamlessly across the two data-centre sites.

In short, VanCity was able to triple the amount of disk space available for data storage, centralize information and backups, and execute its disaster recovery plan more efficiently and effectively. Costs were also reduced – in part, by cutting time spent on administering and managing data storage, and also because the costs of data storage, like almost all things digital, are dropping.

"We are seeing a doubling of performance and halving of prices each year," Fernandes says, adding that cost savings realized by using EMC's network storage solutions can be put towards developing new products and services for VanCity members.

The one potentially weak link in the data storage chain is mobile employees. Fernandes can lead mobile employees to the waters of data backup but he can't make them drink from the backup pool. He makes them aware of the need to backup, and about the risks inherent in not backing up, but he can't do the backups for them. So he does the next best thing: he facilitates backups with a batch file on every laptop.

If the mobile user is connected to the network and double-clicks on the backup icon, the network takes over and a couple of minutes later the backed-up data is part of the central repository of information.

No organization can afford to leave the to-backup-or-not-to-backup decision to its mobile users. There may be too much at stake if a sales representative loses customer orders and contact information or an executive loses a PowerPoint

presentation or vital financial documents.

With 1,200 employees spread out in offices across the country, Export Development Canada needs to ensure the information on employee laptops is backed up regularly. Hardware can be replaced, but data is a whole other matter.

If employees connect to the enterprise network by dial-up or even a virtual private network, backing up can be time-consuming. In addition, the bandwidth issues would be enormous if laptop hard drives had to be backed up in total each backup cycle.

The EDC, the federal government organization that provides Canadian exporters with financing, insurance and bonding services, was looking for an automated, incremental solution, and discovered iFolder from Novell.

Currently, 18 EDC employees are pilot-testing iFolder. "We were finding ourselves challenged with data protection aspects of a mobile workforce and it was becoming an increasing challenge to make sure data was protected and available whether or not (employees) had access to their laptop," says Robert Pettifer, EDC's manager of open systems infrastructure. He adds that he did not want to introduce a complex or time-consuming system that relied on employees remembering to backup laptop data.

With iFolder, backups occur automatically when remote employees connect to the network, so the system is seamless to the end user. If an employee at the airport creates a new presentation or spreadsheet, it is automatically backed up the next time the employee connects to the network to check email. Data is saved on the employee's iFolder folder on the server.

All data transmitted is encrypted for security purposes. Saving on bandwidth, only data that has changed from the last backup is saved during subsequent sessions.

James Simzer, director of field and channel sales for Novell Canada, points to productivity losses if mobile devices die or disappear and the user no longer has access to data. He says resellers who ask pointed questions will be able to help enterprises think seriously about data backup. They add value to their sales when they sell backup systems, but they also add value to the enterprise. The last thing any company wants to do is outfit a group of mobile employees with laptops and connect them to the enterprise only to run into data backup issues after the fact.

Although included with Novell Netware 6.0 and 6.5, iFolder also runs on platforms such as Windows 2000 and Linux. The fact that it is cross-platform means that authorized Novell partners can sell it to customers using almost any network platform. "iFolder opens up doors to discussions around storage management, data access, data security, redundancy and security planning," says Simzer. And that opens the doors to additional sales.

Says EDC's Robert Pettifer: "People use their laptops as desktops. They expect to take their data with them." If a laptop goes missing, or an employee leaves a laptop in the office, the employee can connect to the EDC network from home and access all laptop data stored on the network.

"We want to ensure people can backup their data without meaning to," Pettifer says, acknowledging that it is easier to herd cats than it is to get mobile computer users to set up a strict back-up regimen.

Pettifer knows of what he speaks. Shortly after setting up the iFolder pilot, his laptop's hard drive crashed. He installed a new hard drive and reinstalled his operating system, logged into the network, connected to his iFolder and downloaded all but his last couple of hours of work. "I'm not a consistent back-up person. I could have easily lost four or five months of work," he says.

Asked what happens if the server on which the iFolder data sits were to crash, Pettifer says that, too, is backed up. This does not happen in real time, however, so there is a possibility some data might be lost, but that's a business decision based on cost and the value of data. Not every financial statement would compare to real-time financial transactions that might occur across a network.

What to backup and when to back it up a business issue, not an IT issue, says Blake Genraich, director of sales with Storage Pipe Solutions, an IBM-authorized reseller in Toronto. He explains that the business decision should drive the IT.

Not all companies need to backup in real time. Some organizations can get away with nightly or weekly backups. What gets Genraich are companies that are simply not ready for data disaster. "I'm shocked at the lack of preparation. I met recently with one company – a publicly traded company – whose IT director took the backup tapes home each evening." This left valuable data susceptible to theft or destruction.

When asked why so many companies are not dealing well with the onslaught of data, Genraich is quick to reply that "there's an unwillingness to change and an unwillingness to spend money."

Yet, the consequences can be dire. Genraich says a law firm with 70 lawyers, a 200-person local area network and several servers could lose a quarter million to a half million dollars in lost productivity if the network were to go down for a couple of days. It could be even worse if the data was permanently lost.

The Storage Pipe Secure Service lets companies with small or time-challenged IT departments outsource data backup. The system uses an agent loaded on the target server to send encrypted data via the Internet to the Storage Pipe data facility in Toronto. The company determines what data gets backed up and how often the agent 'wakes up' to run backups. The system is completely automated and there is no capital investment in

data storage infrastructure, Genraich says. Bandwidth isn't an issue for most companies with broadband Internet access, such as DSL or frame relay.

The Storage Pipe agent can also sit on laptops and be set up to backup data a couple of times per day or overnight, depending on the business needs of the people involved.

What Storage Pipe offers, Genraich admits, "is insurance." However, if workforce productivity or a company's survival depend on the ability to recover quickly from a data disaster, it's difficult to dispute the need for data backup and recovery insurance.

But, what price insurance? Medium-sized companies may be looking at a cost of \$1,000 to \$4,000 per month for the Storage Pipe 'electronic vaulting' system, versus a capital outlay of \$10,000 to \$20,000 for on-site backup systems and storage devices. Then they still have to worry about protecting backups against fire, floods and other disasters, as well as theft or vandalism. And they have to maintain the hardware and backup media.

When it comes to selling the need for data backup, resellers have improved over the last few years. But, Genraich says they can do more. It helps their bottom line when they add value, but it also helps the company that would otherwise have egg on its face if it could not recover from a data disaster, he adds.

"The big issues in data management are storage efficiency and risk mitigation," says David Liff, vice-president of BrightStor Solutions with Computer Associates. "The key is don't over insure."

Liff says business needs should drive storage efficiency and risk mitigation decisions, and technological solutions should align data protection costs with the value of data to the business.

As storage capacity increases and the need for backup and rapid recovery becomes increasingly critical, technology solutions must become easier to manage and remain seamless to end users, he says. However, storage capacity is like a superhighway. The more lanes you add, the more it becomes congested.

That happens with data storage because businesses do not properly assess what should be backed up. They simply throw more storage capacity at their ever-increasing data.

"The vast proportion of data is not mission-critical or all that important, but in some organizations all data is stored the same way – on a high-availability solution," he says.

Imagine all the temporary files, duplicate files, redundant files and personal e-mail – archived and long forgotten – eating up disk space in a large enterprise. Liff says 70 to 80 percent of data is temporary, transient or dead.

He advises companies to set data priorities and store what is most critical in the most effective manner. Why spend \$100,000 to protect \$10,000 worth of data? If the human resources department does not have access to data for a day, the company will survive with minor productivity losses. However, losing the ability to process transactional data in real time for even a minute or two can cost a company millions of dollars and also customers. That, he says, is the kind of thinking that should drive data storage, management, backup and recovery strategies.

Channel partners should be involved in the assessment process before selling data storage and backup hardware and applications, Liff says.

In addition to offering BrightStor Enterprise backup and recovery systems, Computer Associates produces tools that let resellers assess data quality before implementing backup systems. Resellers should be able to tell customers which departments are using what data, when files were last used, if there are duplicate files, and which files might be safely discarded or archived on less-expensive storage media, before any data storage and backup business decisions are made.

"Eliminate the deadwood data and help the company save storage and backup capacity," Liff says. "That helps resellers build trust and relationships with clients and gives their client more control over data expenditures."