CANADA'S PREMIER MAGAZINE FOR BUILDING OWNERS AND MANAGERS

Canadian PROPERTY MANAGEMENT

VOL. 19 NO. 1 • MARCH 2004

A Primer for Alternate Network Suppliers

Disaster-Plagued Summer Reinforces Need for Telecom Recovery Plans

By Ian Miles
Toronto Hydro Telecom Inc.

Not in recent history has Canada been beset by so many crises at once. For organizations that rely on information technology to be in business, the events of the past year have been a wake-up call.

When the SARS outbreak occurred in Toronto, organizations scrambled to assess the risk and implement contingency plans. Exposure to SARS within an organization's data centre would have resulted in staff quarantine, potentially shutting down data centre operations for 10 days or more. Isolating staff and moving operations off site were some of the ways organizations sought to minimize this risk.

The threat of fire, although rare in modern office buildings, can be the most difficult from which to recover, destroying both equipment and records and possibly affecting operations for weeks or months. One of the more likely business interruptions is due to power outage. While most modern data centres have access to back-up power sources, the duration of the outage can be problematic. During the August 14 blackout many back-up generators were called upon for several hours and simply ran out of fuel.

But it's not just disasters external to the business that pose a threat to business operations. What happens if a major piece of data centre equipment breaks down? The time to repair or replace the equipment could take days or weeks. In addition, network service can be disrupted if a supplier's cables break or are cut. And then there's the potential for human error. Organizations with disaster recovery plans are able to encounter the unexpected with confidence and emerge from the crisis relatively unscathed.

BUSINESS INTERRUPTION CAN BE CATASTROPHIC

Research has shown that two out of five companies that experience business interruption through natural or man-made disasters will be out of business within five years. Network downtime can be a key factor in a business's demise. The potential cost of network downtime ranges from estimates of $28,000 US per hour for a shipping company, and $90,000 US per hour for a catalogue retailer, to more than $6-million US per hour for a investment brokerage firm.

What about businesses that exist only through networks such as the Internet? Without network service, they are effectively out of business.

To minimize the impact of such events, organizations need to evaluate how dependent they are on electronic transactions and their information technology infrastructure. They need to estimate the financial impact of not having network service for a 24-hour period or longer. And they need to examine the alternatives for ensuring the level of back-up service they require.

It wasn't that long ago that the back up of data simply meant writing data files to tape every 24 hours and physically moving the tape to an off-site storage facility. While this approach may still be adequate for smaller operations, larger organizations often require a more sophisticated strategy.

Most financial institutions, for example, have duplicate data stored off site that mirror their current operations. Under this approach, every transaction is written simultaneously to both the primary and duplicate database, providing an exact replica at any point in time.

Not every business will require this level of data redundancy or duplication. Some may choose to back up at less frequent intervals – perhaps every few hours or once a day. What's most important is that the data is stored in a physically separate location from the company's data centre and can be readily obtained when needed.

For companies that cannot afford to have a disaster disrupt data processing and network service, duplicate facilities are often required. Sometimes referred to as "hot sites", these are physically separate facilities that are capable of replicating the organization's primary data centre operations. In the case of a major equipment failure or power outage, operations can simply switch over to the alternate site with little or no disruption to service.

RELIABLE CONNECTIONS CRITICAL

Companies need to know that, should the unexpected happen, they have dependable back-up network service already in place. For many companies this means choosing alternate network suppliers. Under this approach, if one carrier's network is down the company can quickly switch to its alternate network supplier with minimal or no interruption to operations.

An alternate network supplier must be able to match or exceed the service requirements placed on a company's primary network supplier. For most businesses today that means having access to more than one supplier of high-speed, high-bandwidth network service in the building where the company's data centre is located.

Be wary of any supplier that proposes only a single solution. There are often several ways to meet a business's disaster recovery and redundancy planning requirements and at a variety of price points.

Always ask for complete transparency in any proposed solution. When considering an alternate network supplier for diversity purposes, companies need to see exactly how their network traffic will be routed. Some network suppliers resell other carriers' services so their proposed solution may not provide the diversity required. Ideally companies want to select a carrier that uses only its own fibre-optic network to be assured that the alternate network is truly diverse.

Network reliability in an alternate supplier is crucial. Businesses need to inquire about a network supplier's service standards and track record of availability. Suppliers whose only business is network operations usually have superior network availability because keeping their network up and running is often their top priority.

Be sure to check a network supplier's record of responsiveness to problems. No matter how reliable the supplier, there will be some problems along the way. What's critical is how quickly the supplier responds to service problems and that they provide timely updates on problem resolutions.

Review any Service Level Agreement to make sure it is realistic and doesn't promise service levels that would be impossible to meet. Companies are wise to ask for references and talk to other customers to determine that a potential supplier has a history of delivering on its promises.

With network service contracts lasting up to five years or longer, companies are well advised to assess the stability of any network supplier before signing on. There has been much turmoil in the telecommunications industry. Enter into an agreement with a company that has the financial strength and staying power to be able to deliver on the contract.

Disaster recovery is now a top priority for Information Technology managers and it's likely to remain a top priority, as companies become more and more dependent on information technology to run their operations. Property managers can help tenants implement effective disaster recovery solutions by providing access to more than one high-speed, high-bandwidth network supplier – one that can offer true network diversity and superior network reliability. S

Ian Miles is the President of Toronto Hydro Telecom Inc. Through its wholly owned 450-kilometre fibre optic network, Toronto Hydro Telecom connects more than 400 commercial buildings across Metro Toronto.