

## Disaster planning 101: How to stay connected, no matter what

February 12, 2009 - 4:23pm

<http://www.tele-management.ca/node/9247>

In late 2008 and early 2009 a strike among Ottawa's bus drivers would transform the capital's normally peaceful roads into pretzelled nightmares of cars, transport trucks and frayed nerves. Traffic became a real issue, and suddenly commuters used to spending 20 minutes door to door faced drives that would last an hour or two. By the second day of what would turn out to be a 52-day strike, Jean-Guy Francoeur had had enough.

President of Corporate Massage Therapy (CMT), specializing in registered massage therapy and corporate health programs, Francoeur normally needs just 10 minutes to drive to work. But his commute went awry in hurry. The weather certainly didn't help. "We had the strike and the snowstorm on the same day. I spent a couple of hours on the road myself and, well, that wasn't going to happen again."

Francoeur was prepared. He'd already signed up for phone service with Versature Corp., an Ottawa-based hosted IP-PBX provider. Instead of fighting traffic, Francoeur could make and take business calls directed to the softphone on his laptop PC. He could address corporate e-mail, and generally get on with his work from just about any location, given a good Internet connection. This allowed him to shift his hours such that he wouldn't have to drive to CMT's headquarters until later in the day, when the traffic had subsided. "I work at home until 9:30 10 a.m. – an hour, an hour and a half more than I used to."

Francoeur's story illustrates the issues telecom and IT managers face when events conspire to keep people from reaching the office, or when the office is out of service due to power problems or a natural disaster. Does the company have the tools to continue operating?

Business continuity and disaster recovery are particularly important in this economic climate. Nowadays, no one can afford to miss calls from customers. "From a cost perspective, it's enormous," says Amir Hameed, national leader, application sales and engineering at communication equipment provider Avaya Canada. "We're in a global environment...If you're not there, customers will go elsewhere at your expense."

Communication system providers have been working to ensure their equipment addresses this concern – but not all solutions are created equal. We've looked into the business continuity features of Avaya Inc.'s, Microsoft Corp.'s and Cisco Systems Inc.'s equipment to help IT and telecom managers assess which method would work best for their companies.

### Avaya's survivability

The shift to IP as the underpinning communication technology for most new phone systems has proven to be something of a paradox for business continuity planners. On one hand, IP lets companies consolidate their communication system into a single entity – one box supporting call routing across the entire enterprise, no matter where the branch offices might be in relation to HQ. It's efficient. But what if the main office goes offline? Lacking proper planning, a business could find that its branch bureaus go down with the main ship, and suddenly no one has a dial tone.

Avaya, for one, has designed its communication systems to work independently if headquarters goes offline. When the connection between the main office and a branch office is severed, the gateway device located at the branch takes over, providing the same features and functions as the main system.

"We actually mirror the software so everything from unified communications to call centre functionality is kept at each location," Hameed says. It's known as a survivability feature. Avaya's system also provides connection-preservation failover functionality, which essentially means people engaged in a conversation wouldn't lose the connection mid-sentence. And if the customer has implemented the communication system to balance the workload among numerous branch offices, that aspect continues if the main site becomes inaccessible – the gateways take over the load-balancing duties.

For businesses like CMT that incorporate teleworking into their business continuity plans, Avaya takes things one step further, using VPN software to enhance its 4600 series IP phones. The moment a user plugs the phone into an Internet connection, the software tunnels through to the corporate network and begins acting as if it were the user's main office extension. This simplifies the telework situation. "Executives love the VPN phone because it's less work for them," Hameed says. "They plug it in and it works."

### The Microsoft way

As a software company with interests across the full IT spectrum, Microsoft seems to take a dual-sided approach to business continuity. "There are a couple of levels you have to think about," says Bryan Rusche, Microsoft Canada's unified communications product manager. "One is data....The other is application availability."

On the data side, Microsoft has designed its systems to continually update any backup equipment on the fly, so if the main box goes offline the backups wouldn't miss a beat. Local replication functionality copies e-mail messages in a separate location on a Microsoft Exchange Server, for instance, affording continuity in case of hard drive failure. Failover features for server clusters allows mailbox and e-mail data to be accessed on a second server located in the same building. It works automatically, which is both good and bad. "Because it's actively monitoring for that situation, it can't be geographically dispersed," Rusche says, adding that some Microsoft partners offer stretch clustering capabilities for more dispersed situations, although that's not a standard Exchange feature.

For companies using complete secondary office sites in their business continuity plans, the standby service in Exchange – a relatively new feature – does enable mailbox data to be replicated on a server off site, so if the data centre goes down, the company's e-mail system doesn't. Unlike the clustering capabilities, this isn't automatic – an administrator has to flip the switch to make it happen.

"It saves customers a huge amount of money in tape backup," Rusche says, noting that restoring operations from tapes can take more time, and also requires investment in an entirely different infrastructure.

Companies can configure Microsoft's Office Communications Server (OCS) – the VoIP part of the Microsoft unified communications suite – for load balancing and failover across server pools as well, so the voice connections stay up even if the main OCS server goes down. As for the application side, Microsoft's Outlook e-mail client and the Communicator voice, video and instant messaging program both feature built-in VPNs, giving users access to all of their communication features remotely, should workers have to work from home during a disaster. And of course businesses can deploy Outlook Web Access so users can gather their messages from any Web-connected computer. "In something as simple as a snowstorm, the ability to connect at home and have access to all of your communications is hugely beneficial," Rusche says.

#### Cisco's down scope

While Microsoft talks up data and applications, Cisco focuses on the resilience of the underlying data network as a fundamentally important aspect of business continuity. The company's well-known IOS system for routers and switches incorporates call control functionality, so as with the Avaya equipment, Cisco's branch office gateways can pick up where the main site left off and users can continue to communicate. "We're always sure to identify potential single points of failure," says Francois Thibault, Cisco Canada's regional sales director for unified communications.

But where, exactly, those points of failure reside vary from customer to customer. For some, the single-HQ/ multiple-branch architecture is the lynchpin, while for others distributed, load-balanced contact centres play a major role. Information security matters to most as well.

To identify each client's weak spots Cisco has a set of blueprints targeting different parts of the communication infrastructure – the network itself, security applications and procedures, third party software, and call centre software.

"In 80% of the cases, that's the part that requires the most preparation," Thibault says. Call centre performance directly impacts customer relations and company reputation.

One fact that informs business continuity planning is the interconnectedness of communication systems. More so than ever before, the myriad pieces of a company's communication

platform speak to each other – voice mail and e-mail systems share data, voice and instant messaging work hand in hand, branch office phone numbers are merely extensions on the main system. Does this simplify business continuity, or make it more complex?

Thibault says he figures interconnections streamline things. "It offers you a lot more choice. Now the common link is IP and it's a standard. In the past, you had a voice mail system from one manufacturer that might not speak to others."

Hameed from Avaya agrees. Lacking interconnectivity, it would be more difficult to employ advanced features such as smart call forwarding and presence, which rely on the communication system being able to understand where the user is and how he wants to be contacted. That's the magic behind single-number reach. "It allows me to get my job done irrespective of where I am," Hameed says.

#### IP network planning

But looking at interconnectivity another way, it could complicate matters. John Glover, head of Mayne Island, BC-based telecom consultancy MayneStay Consulting Group, points out that the number-one culprit for communication failure is improper IP network planning. "Now that we're on the verge of abandoning TDM, there's an increasing requirement to make sure the IP infrastructure is not only solid to give you the quality of service you require, but also highly resilient," he says.

At issue is the fact that IP carries both voice and data on a single network. Too often, businesses as much as cross their fingers hoping the system will provide high quality of service. "Organizations fail to stress test the infrastructure," Glover says.

That's a surprise, because most communication systems manufacturers offer IP network testing as a standard prerequisite to implementing IP phone systems. Still, in Glover's experience few businesses bother with testing.

Those that do test the infrastructure sometimes find interconnectivity isn't worth the hassle. Instead of combining voice and data on a single network, they operate two IP links – one for voice, the other for data. Glover says there are two benefits here: first, quality of service tends to be better; second, it adds an extra layer of business continuity protection. "They'll have two gateways, so if one fails they might be able to use the other one."

Glover says many businesses don't make business continuity planning a priority. But others disagree. "When I'm talking to customers, business continuity always comes up," Hameed says. It's no surprise. "Look at the experiences we've had. We had that massive blackout, the outbreak of SARS, we heard about the avian flu. In the US we saw Hurricane Katrina. How are we protecting ourselves and our business interests?"

Francoeur, for one, seems to be protecting his business. Since he started using Versature's IP phone service back in December, he has rolled it out to CMT's managers as well, who now also

telework for part of the day. It not only saves them the hassle of fighting rush hour traffic during the transit strike, but it also allows them to focus on business tasks that require concentration.

"We've already changed the schedule to make that permanent," Francoeur says. "On a short term basis, they don't get to work from home for a full day. That's when things might not be as productive." But when managers work at home for part of the day, "that's where I've seen more productivity."

## Sidebar

### Avoiding telework disasters

Companies in the Ottawa area had to scramble to support teleworkers when the transit strike began in early December. Commuters faced long drives and often decided they'd be more productive if they worked from home instead. According to telecommuting experts, there are certain best practices to follow – and pitfalls to avoid – for true work-from-home success.

For instance, consider the home office environment. According to Bob Fortier, president of InnoVisions Canada, an Ottawa telework consultancy, the space should be quiet, well lit, and it should be a comfortable place to work for an extended period of time.

It's also important to ensure the home office is safe – that the electrical outlets aren't overloaded with computer equipment, for example. "Companies are liable to make sure they don't send their employees to work in harmful conditions," Fortier says.

Then there's the home-computer conundrum: if an employee uses his home PC, how does an employer know the computer is virus-free and protected against hackers? Some organizations give workers company-owned laptops to avoid the question. These issued machines undergo a rigorous protection process, so by the time employees get to use the computers, there's very little chance that the PCs can be breached.

But it's not always necessary to insist that employees only use company-specific laptops. "It depends on the way they want to go," says Paul Emond, president of Versature, an Ottawa-based IP-phone service provider. "If you're using a hosted service such as LogMeIn, your home PC is just a window into the office PC, so there isn't as much of a risk of introducing viruses into the office network."

Introducing telework to the company's human resources policies can be a significant challenge. For some, working from home leads to one question: "How do I know the employee is actually working?"

"I can see where they're coming from," Emond says, noting that as a small-business owner himself, he can't afford to float unproductive workers – everyone needs to pull their weight.

He notes that some VoIP phone systems allow employers to review employee call records as a way to track productivity. "This is the kind of thing people do for office-based employees all the

time – you can do the same for your home-based employees."

At Corporate Massage Therapy, an Ottawa company using Versature's hosted IP-PBX for telework, performance is a matter of trust. "Most people, if they enjoy what they do, they're going to be productive," says Jean-Guy Francoeur, CMT's president. "They're not going to sit there and do nothing. That's why they work."