Remote Access

It's not a lifestyle choice, it's a critical part of disaster recovery.

Scott Welch

By Scott H.E. Welch

Imagine waking up to a call tomorrow morning from the local emergency services department informing you that there was a chemical spill at your work and that all access to the premises would be closed for aprpoximately 24 hours. In addition, all the power at your offices would also be shut down. The managment team and all its employees would be forced to stay at home and work. But, how effective would this be if a number of them could not access your company's network?

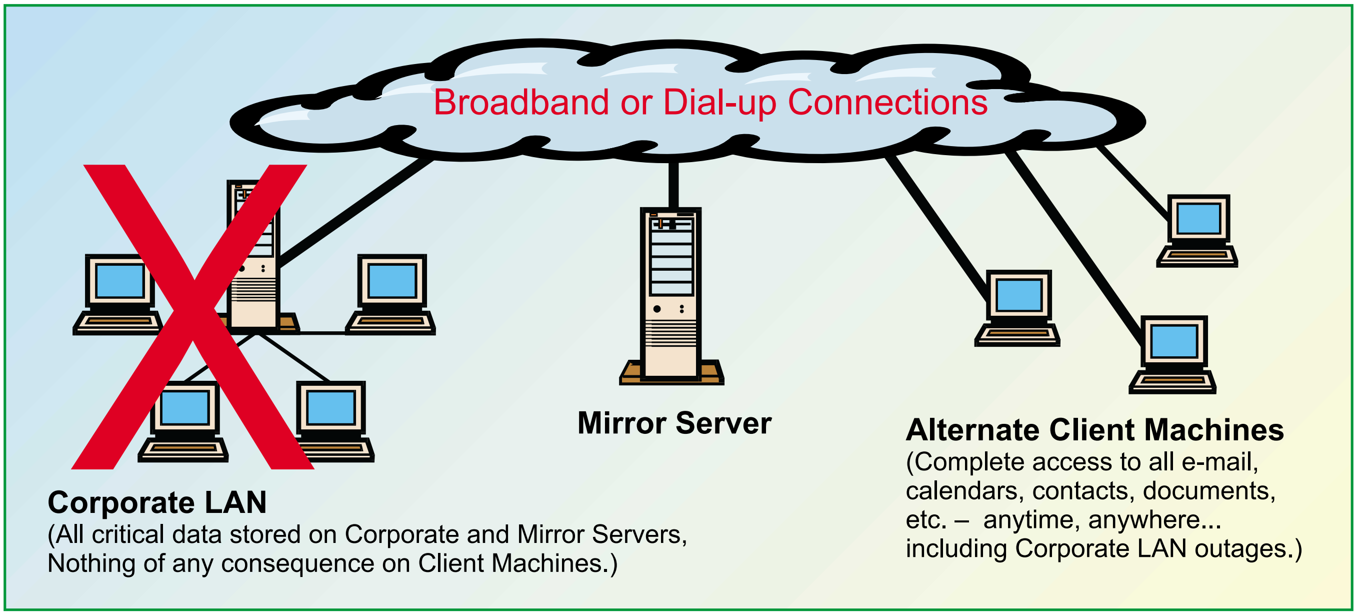
Now take just a few more minutes and imagine that instead of a chemical spill lasting a few hours you were dealing with an emergency that would take days or even weeks to recover from. In fact, in the case of an extreme emergency, such as a fire, your entire IT infrastructure may be destroyed.

Is your organization confident that in the face of these potential disasters that it would still be business as usual? Probably not. In all of these scenarios, the critical question for IT managers in charge of disaster recovery is how long it will take to get back up and running, and how much data your end users will lose.

In the past, providing remote access to computing services was seen as either a lifestyle choice, for employees who wanted to work from home, or a tool that was only required for "road warriors" such as salesfolks. Since September 11th, though, more and more companies are realizing that remote access is a critical component of disaster recovery. When considering remote access solutions, there are actually three separate issues that you have to look at: the ease of deployment, the bandwidth requirements, and end-user results.

The other critical issue to examine is whether your disaster recovery / remote access solution takes into account the fact that your users may be running on completely new computers. Any solution that assumes end users keep their machines is not a solution. There are numerous scenarios in which end-user machines are rendered unusable, from simple emergencies that cause users to flee the office to the unthinkable, such as a fire or terrorist attack. In any of these events the critical result is that the end users are unable to access their regular machines. They will have to be able to continue their work without ever having access to their old machine.

Of course, this ability to work from alternate machines also means that for the more standard case of users working from home remote access is much more painless.


Broadband or Dial-up Connections
Mirror Server
Corporate LAN
(All critical data stored on Corporate and Mirror Servers,
Nothing of any consequence on Client Machines.)
Alternate Client Machines
(Complete access to all e-mail,
calendars, contacts, documents,
etc. – anytime, anywhere...
including Corporate LAN outages.)

“During recovery ... your users may be running on completely new computers.”

Instead of lugging a laptop home every night, your users should be able to just use the existing machines that they have at home.

A Real-world Example

As a real-world example, let’s look at providing remote access to your messaging system. As e-mail becomes more prevalent, more and more of your employee’s business is being conducted by email. In addition, your email system is probably used as a contact management system, which means that your employees are likely to need access to the data in the messaging system for other communications tasks, such as making calls and sending faxes. Finally, chances are pretty good that this same system is your primary calendaring system as well.

Put these together and it’s clear that providing good remote access to these applications will go a long way to allowing your company to recover from a disaster.

As you choose your software, you will need to be thinking about the implications for remote access and disaster recovery. For example, many popular email applications, such as Microsoft Exchange, store each user’s mail out on that user’s computer. It’s a sad fact that if those computers are sitting in the office with the power turned off, the best software in the world won’t help the user get at their content. So, it’s critical to make your chosen vendor demonstrate what is involved in accessing user content from alternative machines.

Next, you have to think about the end users and the training that they require. In a perfect world, the remote access solution you choose will provide users with exactly the same user experience and user interface that they are familiar with. In a disaster, they are already going to be dealing with extraordinary pressures; the last thing you need is for them to have to learn a new way of working. Also critical at this point is to ensure that the remote access solution provides full functionality. At least one major email vendor has a remote access / web “solution” that allows users to read their mail – but that’s it! No forwarding, no replying, no composing and sending.

As if these issues are not enough, next you have to contend with network bandwidth. If all of your users had 10 Mb to their home, and you had a remote emergency facility with a T-3 backbone, life would be fine. Sadly, the majority of your users will be connected at modem speeds, with only a few at broadband. If you have to set up an emergency facility, you’ll be lucky to get even T-1 speeds. Hence, it’s vital that your remote access solution does not depend on broadband connections.

The upside of all of this planning is that if you have implemented your system correctly, your users will be able to use any machine on your network to access their email, contact information and calendars; they will be able to work from home or on the road; they will be able to replace their machines without requiring your intervention; and to top it all off in the event of a disaster will be able to work from any remote location and any machine that you provide them.

Putting vendors to the test

One quick safety tip: Vendors are often quick to claim that their software will meet the criteria set out above. The question is, do their claims hold up? Fortunately for you, there is an easy way for you to verify their claims: Take one of your laptops, make a dial-up modem connection to the Internet, and sit them down in front of your machine and tell them to access their own messages, contact information, and calendar. It should be easy, right? TUG

About the author: ***Scott H.E. Welch*** *(scott@centrinity.com) is Chief Evangelist of Centrinity, Inc., developers of the FirstClass® communications system. He invites your comments about security and system architecture.*