

The Role of Wireless Technology in Disaster Recovery

Until recently, most organizations considered wireless technology to be an alternate workstyle, not a linchpin of their IT strategy. But wireless technology has matured, and today there are a number of systems and technologies available that make wireless a reliable solution for both day-to-day use and emergency backup.

Perhaps the event that best illustrates the resilience of wireless technology was the terrorist attack of Sept. 11, 2001. While wireline phone networks in the New York area were rendered virtually useless in the wake of the attack, people in the affected areas were generally able to use wireless devices to maintain contact, at least for data if not voice communications.

Wireless voice networks, while not completely incapacitated, were overloaded, making it nearly impossible to get a call through. However, wireless data tools such as Blackberry and cellular short messaging services (SMS) provided an avenue to keep the lines of communication open.

In addition, for many companies whose facilities weren't destroyed, but were inaccessible for days or even weeks, wireless access offered the only way to recover critical data from stranded servers and maintain basic business functions.

The resilience of wireless networks -- coupled with the prevalence of mobile devices -- positions wireless technology to play an integral role in the emergency response plan of most organizations.

Components of Wireless Disaster Planning

In the event of an emergency, the first order of business is going to be finding and maintaining a connection with the organization's key people. Fortunately, many of these personnel already carry a variety of wireless devices, including pagers, data-enabled cell phones and PDAs.

A good initial step in developing a wireless emergency plan is to keep the contact information for the mobile devices used by critical personnel ready as part of your emergency response system. And for those key people who don't currently use wireless devices, it's worth considering supplying them with at least one, and preferably two, for use in an emergency.

Of course, the definition of just who is critical will vary depending on your corporate structure and the nature of your business. But at the very least, you'll want to ensure access to the senior executive team, lead IT personnel, and probably one senior representative from each significant functional area, such as customer service, operations, finance, etc.

The next thing to consider is establishment of a wireless LAN. The technology has advanced to a degree that a fixed wireless solution can reasonably be considered a reliable backup for a data network. With transmission speeds as high as several hundred megabits per second, these networks have the capacity to handle the kind of data traffic you're likely to generate in the event your wired LAN goes down. And because fixed wireless technology provides a dedicated network, you don't have to worry about the kind of system overload that can affect mobile wireless networks when demand soars.

A second point to consider is whether your data could become stranded should your facility be inaccessible. Of course, you should think about maintaining a backup data store at a location separate from your main facility. But in addition, you might want to establish a remote worksite where key employees could gather to handle the functions needed to keep your business in business through the duration of the crisis. This can be accomplished through use of a fixed wireless network. These point-to-point networks work over a limited geographic range -- up to 40 miles with repeater antennas -- making them a good solution for linking two work sites together.

The Security Question

The general perception is that wireless networks are inherently less secure than their wired counterparts because wireless signals are vulnerable to interception. While some concern is warranted, most experts contend that wireless networks can be made adequately secure for most uses by following a few simple measures.

First, many organizations don't even utilize the security features provided with their systems. Employing 128-bit encryption and spread-spectrum technology -- which breaks the encrypted data into disparate chunks for transmission and reassembles them on the receiving end -- data traveling over a wireless LAN can be as safe, or safer, as data traveling over any remote wireline connection.

The Bottom Line

Wireless technology provides a viable, cost-effective resource for disaster management and recovery. In outlining the role of wireless technology in your firm's disaster recovery plan, it's important to keep in mind the capabilities of each specific technology. For example, while cell phones and PDAs provide an excellent way to deliver short messages to people who are on the move or scattered in various locations, these tools are still inadequate for manipulating large quantities of data or accessing complex Web pages.

By incorporating a broad scope of wired and wireless technologies into your disaster recovery planning, you can ensure a measure of data and network redundancy, giving your organization an edge in the event of a catastrophe.

By Dale Windle

Dale Windle is senior business continuity and disaster recovery consultant and project manager with DisasterRecovery.com, a vendor-independent company specializing in business continuity and disaster recovery planning. DisasterRecovery.com provides consulting services, seminars and continuity planning software to hundreds of clients around the world. Dale can be reached by email at: sales@disasterrecovery.com