

[Register/Subscribe](#)  
[Home](#)

BusinessWeek online

Video Views

BusinessWeek online

[Close Window](#)

APRIL 8, 2003

SECURITY NET

By Alex Salkever

## Don't Put All Your Data in One Basket

**The biggest threat isn't a hacker -- it's a fire, flood, or a physical attack. Be sure you have genuine backup and the right kind of redundancy**

Baghdad's telecommunications infrastructure fell silent during the first week of April under a rain of precision-guided bombs. U.S. and British planes targeted phone facilities and other critical pieces of the Iraqi communications infrastructure, mirroring campaigns in Afghanistan and the first Gulf War to isolate the leadership from the levers of power.

CEOs in the U.S. needn't worry about an F-15 taking out their data connections. And it's also clear that firewalls, antivirus systems, and other digital protective gear all have their places in the best-laid plans to safeguard a business. That said, the U.S. military chose to use bombs -- not hackers -- to drop Iraqi networks for a reason. Nothing brings a network to a halt more easily and quickly than physical damage, whether it be from a plane hitting the World Trade Center, massive floods in Texas, or a high-temperature chemical fire on a train passing through a Baltimore tunnel filled with fiber-optic cables.

**TELECOM "HOTELS."** Yet as data transmission becomes the lifeblood of Corporate America, most big companies haven't performed due diligence to determine how damage-proof their data lifelines really are. Only 20% of midsize and large companies have seriously sussed out what happens to their data connections after they go beyond the company firewall, says Peter Salus, chief knowledge officer of MatrixNetSystems, a network-optimization company based in Austin.

The collapse of the World Trade Center left most of Lower Manhattan, the epicenter of the global financial system, without data connections for a week or more. Many of the affected companies thought they were covered for any eventuality, having contracted for not one but two high-capacity data connections from their offices.

Redundancy doesn't help much, however, if your Sprint ([FON](#)) and AT&T ([T](#)) connections pass through the same geographical location. "There were a lot of cables and suppliers that terminated on West Street or World Trade Center 7. They were wiped out," explains Salus, who adds: "If you were on WorldCom, which came out of Midtown Manhattan, you didn't notice a thing."

**TWO INTO ONE.** All the more reason for companies to make sure that the data connections they rely on for security aren't stored in the same building and vulnerable to the same threats. Unfortunately, massing huge chunks of connectivity in so-called "telecom hotels" is the norm. "We go physically visit the site. You'll often find 40 or 50 different carriers in the same building," says Jonah Yokubaitis, CEO of Texas.net, a large Internet service provider with 1,000 business customers in the Lone Star State.

When networks are less diverse and alternative pathways from Point A to Point B are far more limited, most of the risk is in getting data out of the local loop, he says. Once the information leaves the

telecom hotel, data carriers often carry traffic across shared strands of fiber. Says Yokubaitis: "You need to make sure both of your connections don't run over the same fiber path. You may be dealing with different companies, but the fiber may be going over the same natural conduit."

Here's what smart companies can do to minimize risks: First, chief technology officers can run a simple trace-route check. This basic piece of software sends out a package of data and watches its path. "If [the data] go through the same set of Internet protocol numbers [unique numbers used to identify each device on the Internet], then you're going through the same place, even if it is someone else supplying the stuff," says Salus.

**THINK LOCAL.** Second, visiting co-location facilities where your data carrier houses its equipment is key. Finally, make sure vital locations can continue to function even if they lose their Internet connection to the outside world. That means placing servers containing copies of key software and company data on local networks at different locations. "In those highly critical areas, you probably want to be redundant, without the need of external communications," says Paul Mockapetris, a key architect of the early Internet and chief scientist and chairman of Redwood City (Calif.) software concern Nominum.

The upshot of all this? Fires or floods or, God forbid, another terrorist attack are all genuine possibilities, and a byte of prevention is worth a megabyte of cure.

---

[Salkever](#) is technology editor for Business Week Online. Follow his column every week, only on BW Online

*Edited by Douglas Harbrecht*

Copyright 2000-2003, by The McGraw-Hill Companies Inc. All rights reserved.

[Terms of Use](#) [Privacy Policy](#)



A Division of The McGraw-Hill Companies

The McGraw-Hill Companies