

SPECIAL REPORT

Disaster Recovery and Business Continuity

Insuring the Safety of Your Network

FREE

from
nwfusion.com

by

Network World Editors

Sponsored By:

Quantum

 **BROCADE**

Produced By:

NetworkWorld

www.nwfusion.com

QUALSTAR
The Tape Library Experts

EMC²
where information lives

availability.com
IT starts here

The terrorist attacks on the World Trade Center and the Pentagon last September have catapulted Disaster Recovery and Business Continuity procedures to top-of-mind status among network executives. Worst-case scenarios are being prepared, and appropriate preemptive plans are being formulated to guarantee the safety and backup of corporate data, and to insure the uninterrupted functioning of the network infrastructure.

These six articles in Network World's Special Report on Disaster Recovery and Business Continuity will provide you with critical need-to-know information on how to prepare your network beforehand in the event it is the target of a major physical or electronic attack.

Table of Contents

Lehman Brothers' network survives.	3
Investment giant doesn't miss a beat after IT headquarters is leveled in WTC attack.	
Disaster recovery: Then and now.	4
Companies are looking beyond tape backups and hot sites, and toward "business continuity plans."	
Security takes center stage	7
Doors that were usually left open prior to Sept. 11 at Precise Software in Dallas are now locked.	
How ready are the nation's networks?	8
Service providers say their network readiness prevented widespread disruption Sept. 11...but they're still doing more.	
Planning for the worst: bring in the best	10
Expert advice is available for drawing up disaster-recovery and business contingency plans.	
Spending shifts	11
The events of Sept. 11 have caused many IT executives to shift their spending priorities in 2002 toward disaster recovery, security and videoconferencing.	

Lehman Brothers' network survives

• BY SHARON GAUDIN

Moments after American Airlines Flight 11 slammed into the Tower One of the World Trade Center, Bob Schwartz, managing director and CTO of Lehman Brothers, looked out his 40th-floor window to see the roofs of nearby buildings on fire and pieces of his own building raining down. In the lobby outside his office, water was shooting out of the elevator banks.

Minutes later, Schwartz and his managers began moving their workers - the core of the global investment bank's IT staff - down the stairwell, away from the fire and chaos, as well as from the network that kept the company running.

As he made his way down the stairwell, the only thing Schwartz had with him to trigger Lehman's disaster plan and alert the company's CIO, working in London that day, was the BlackBerry pager in his jacket pocket.

"The BlackBerries let us e-mail back and forth, and our colleagues in the New Jersey office told us what was going on," says Schwartz, who made it out of the tower 30 minutes before it collapsed. "From the stairwell ... we decided to trigger the disaster-recovery plan, open up a command center and put voice bridges in place for conference calls."

All but one of Lehman's 625 IS employees, who worked on floors 38 to 40 of Tower One, made it out alive.

And despite the devastation, Lehman's treasury department moved to the back-up recovery site - the day of the attack - and performed its cash-management functions. The day after the attack, the company was trading fixed-income products and had 400 traders online to handle equities when the New York Stock Exchange reopened the next Monday.

"The network was the hero," says Schwartz, who adds that all their pre-planning and network buildup paid off. "No information was lost. I'm sure there were a couple little things here and there, but nothing that interfered with our ability to provide service to our customers."

A network destroyed

Along with the human toll, Lehman suffered a devastating blow to its offices, computer network and infrastructure. Lehman's worldwide headquarters were in Manhattan, with offices in four buildings in the World Trade Center area. The IT department - application developers, engineering teams and the technology management team - was housed in Tower One, and Lehman also had people in three buildings in the World Financial Center next door.

All the desktops, servers and other hardware in Tower One are now rubble, and the other three buildings are unusable as well. In all, the company lost 5,000 desktops, an entire data center and all its networking gear.

Schwartz says the company has not put a figure on the losses the company suffered Sept. 11. But whatever it adds up to be, the financial hit would have been multiplied if the company's lifeblood, its information, had been lost.

"In the planning process, you can never guess what the disaster might be," Schwartz says. "It's always hard to picture what's going to work. We

were cautiously optimistic we would be able to restore all the important applications on a timely basis."

Preparing for disaster

"We had completely redundant networks on both sides of the river," Schwartz says, referring to his offices in Manhattan and the back-up site in Jersey City, N.J. "Every application that ran in New York also ran in New Jersey. All wide-area links were completely duplicated. We had two lines, one terminating in New York and one terminating in New Jersey. When we lost access to everything in New York, we still had access through New Jersey to all our other 45 branches."

Schwartz says Lehman also had two identical data centers, one in Manhattan and one in New Jersey, linked by fiber-optic cable running under the Hudson River. Backups were automatically performed - one center backing up the other - so each set of backups would be remotely stored from its original site.

"We were prepared for the loss of either one of those two data centers," Schwartz says. "When we were attacked, we were able to increase the amount of bandwidth ... allowing us to keep all of our other offices up and running. They were able to continue their normal operations as if nothing had happened."

In the days after the attack, the disaster-recovery team began rebuilding the company's IT infrastructure. Vendors such as Compaq pitched in and quickly shipped the hardware and software Lehman needed. In the first three weeks, Compaq had shipped the company 2,500 PCs.

The disaster-recovery team created a trading facility in its former New Jersey data center.

It also worked out a deal with Sheraton Manhattan, taking over the hotel and removing beds and moving in desktops to give people a place to work. The hotel's ballroom became an IT hub with VPN connectivity to New Jersey.

"We were able to almost immediately seat the most critical people to get the business back up and running," says John Manville, manager of networks and telecommunications, and a senior vice president at Lehman Brothers.

Introducing the ATL M1500

The first scalable, stackable tape backup solution that grows with your business.

Few Things are this Reliable.

Sign up today for a FREE Disaster Recovery seminar at www.NetworkStorage.com

Quantum

Introducing the ATL M1500 - the first scalable, stackable tape backup solution that grows with your business.

Disaster recovery on the run

TUESDAY, SEPT. 11

- 1 8:48 a.m.** American Airlines Flight 11 hits Tower One of the World Trade Center.
- 2** Minutes later, Lehman Brothers' CTO Bob Schwartz and his co-workers head down the stairwell.
- 9:03 a.m.** United Airlines Flight 175 crashes into Tower Two of the World Trade Center.
- 3** Schwartz uses his BlackBerry to alert workers in New Jersey to fire up the disaster-recovery plan while he heads down the stairwell to escape the building.

Schwartz uses his BlackBerry to update Lehman's CIO, who was in London.

Lehman's disaster plan goes into effect and the command center was opened in New Jersey while Tower One was still being evacuated.

- 4 9:40 a.m.** Trading on Wall Street was called off.
- 9:45 a.m.** Schwartz makes his way out of the building.
- 9:50 a.m.** Tower Two collapses.
- 10:29 a.m.** Tower One collapses.

Later in the day, Lehman's treasury department moves into its back-up recovery site in New Jersey and perform its cash management functions.

WEDNESDAY, SEPT. 12
Lehman's fixed-income trading was up and running.

MONDAY, SEPT. 17
Lehman was back doing equity trading when the New York Stock Exchange reopened.

"The network was the hero"

Lehman Brothers' CTO Bob Schwartz largely credits the redundancies in the network for keeping the company running after the terrorist attacks. The company's 5,000 desktops in Manhattan were spread out through four sites -- one in the World Trade Center and three in the World Financial Center next door. A site in Jersey City, N.J., mirrored the Manhattan network and backed it up. After the attack, the New Jersey site served as disaster-recovery headquarters, as well as a trading facility. Lehman took over the Sheraton Manhattan, turning bedrooms into offices and using the ballroom as an IT hub with VPN connectivity to New Jersey. The company also used its London data center to back up some of its more critical applications.

PREVIOUS BACKUP

Back-up site
NEW JERSEY

Fiber link

Data center (World Financial Center)

Tower One WTC

NEW YORK MANHATTAN

DISASTER BACKUP

Back-up site
NEW JERSEY

VPN CONNECTION TO DISASTER BACK-UP SITE

NEW BACK-UP LINK

Tower sites after collapse

Manhattan Sheraton

Data center (World Financial Center)

NEW YORK MANHATTAN

LONDON DATA CENTER

Manville says the company is now running on a single data center and working on setting up another one so it can once again have needed redundancy. Today, it is relying somewhat on its London data center, taking advantage of its spare capacity over a wide-area network. "It's giving us a site to back up some of our more critical applications," Manville says.

And Lehman remains committed to keeping its operations in Manhattan. The company announced recently that it was purchasing a 1-million-square-foot office tower on Seventh Avenue to serve as its new headquarters. ■

Disaster recovery then and now

• BY JOHN FONTANA AND DENI CONNOR

From his office in lower Manhattan, Alen Teplitsky has a clear view of where the World Trade Center towers once stretched into the sky. Today, with the buildings in rubble, he sees a constant reminder of a new world.

Teplitsky won't ever forget the human loss and property destruction from that tragic day in September, but as he moves forward he continues to ask himself: Could our company recover from such a direct attack?

"We had a straight-on view of the World Trade Center, and you have to know now that anything can happen. We're taking that very seriously," says Teplitsky, a network administrator for a phone company that serves the Northeast.

Teplitsky says it's not only the loss of systems, but also the loss of the building that houses those systems and the people who run them.

"Before, if we planned that our whole data center would be destroyed people would have said we were crazy," he says. "But that's what we are doing now."

It's the same "crazy" notion that so many network executives are now thinking about and acting on.

More than backup and recovery
The conclusion many are coming to is

that disaster recovery includes a lot more than the type of backup and recovery that involves tapes and hot sites. They're realizing disaster recovery is only part of what should be a companywide business continuity plan.

Gartner estimates that 85% of large organizations have some sort of disaster-recovery plan, but that only 25% of them have a broader business-recovery plan, and only 10% to 15% of those are up-to-date.

"This tragedy has awakened boards of directors and CIOs to business continuity planning," says Donna Scott, an analyst for Gartner. "The thought process is to expand the planning for loss of life and destruction of property. Every company was unprepared for that."

John Glenn, a certified business continuity planner, agrees there has been an awakening.

"What corporations typically have done is focus on IT at the expense of the rest of the business," he says.

Glenn says business continuity planning is a three-step process:

- * Conduct an analysis that defines an organization's critical business functions, identifies and prioritizes risks (such as natural disasters or terrorist attacks) to those functions, and establishes policies to avoid or mitigate those risks.

- * Devise a disaster-recovery plan for critical systems and data, including: establishing primary and alternate recovery teams; setting up notification procedures such as call trees; determining primary and alternate meeting sites; tracking inventories of software and hardware; having readily accessible contact information for vendors; and clearly defining backup and recovery techniques.

- * Set up intervals of training and testing for the disaster-recovery team and the business continuity plan as a way to make revisions and stay confident the plan is battle tested.

Some may see such extensive planning as merely a fire drill in the wake of tragedy, but history bears out the importance of a business continuity plan. Consider Hurricane Andrew, which struck in 1992 and is the worst natural disaster on record. Within two years, 80% of the affected companies that lacked a business continuity plan had failed, according to the Federal Emergency Management Agency.

The events of Sept. 11 have shown companies just how narrow their planning may have been.

"People were not taken into account. Are people still alive? Do they have the mental capacity to work?" says Rich Corcoran, business recovery information manager for Eastman Kodak and one of the most respected IT executives in the continuity-planning field. He has spent 15 years crafting Kodak's continuity plan.

Corcoran says other planning deficiencies were workstation recovery and detailed plans to store and recover vital records, such as those on microfilm or digitized.

Kodak's plan ensures 100 fully functional workstations are available in 24 hours and 300 within three days. And the recovery time for Kodak's enterprise resource planning (ERP) application is four hours for basic availability and 30 hours for total restore. "That is an extremely aggressive ... plan," he says.

Tom Kelly, senior director of customer services for SunGard, a leading

business continuity services firm, says a major deficiency he saw was in the scope of planning. "We've been having a lot of discussions with clients on business dependencies," he says. "Many hadn't thought that through. Peripherals, such as printers, were commonly overlooked."

Setting a new course

Zamba Solutions, a consulting firm, had basic contingency plans such as telephone lists, vendor contact numbers and data backup, but now all that is under review as the company develops a formal written plan.

"The organization as a whole now recognizes that some sort of plan has to be in place. We have a lot of visibility with upper management," says Tom Booth, director of IT. "The work is less on disaster recovery right now and more on business continuity planning."

Booth is helping define 10 to 12 of Zamba's core business processes, such as payroll and benefits coordination, and the internal and external dependencies on those processes that are key to sustaining the business during an emergency.

"It's an eye-opening experience just to do the dependencies for payroll to figure out all that is needed to get that up and running again," he says.

He says the biggest realization is "that this is more than a systems problem."

That realization happened in June for Rich Obrecht, the IT representative for the disaster-recovery team at a leading oil and gas company in Texas, when Tropical Storm Allison paralyzed Houston.

"We've started to form disaster-recovery teams by business unit," Obrecht says. "We've had fairly lengthy interviews with the business unit people to discuss what they need when an emergency hits, when you don't have an office and you've lost paperwork."

The questions are "Where is my engineer, my accountant? How will they get data, tools, mail? We are just realizing how big this animal is," he says.

Pat Parker, director of data systems for CBS Marketwatch.com, says the notion of property loss is changing how the news organization inputs and replicates data between three data centers in New York, Minneapolis and Redwood, Calif.



Brocade
Conference
2002

JUNE 2-5,
2002,
IN LAS VEGAS

REGISTER BY
MARCH 15TH
SAVE \$200

[Brocade Conference 2002](#)

Survival plan

Consultant John Glenn says corporations should go through a series of basic steps to get rolling on the creation of a business continuity plan:

- Identify key business units, the functions they perform and how critical they are to the overall business.
- Specify tools — such as office and production wares, workstations and communication products — needed to perform business unit functions. Identify suppliers.
- Pinpoint risks — man-made, natural or technological — to business unit functions.
- Develop risk/avoidance and mitigation recommendations, and rate them by effectiveness.
- Create a disaster-recovery team with a reporting structure based on a hierarchy, and define team members by assignment.
- Specify a procedure for declaring disasters that have some forewarning (such as a hurricane) and those that do not.
- Create a non-employee notification list, including vendors, and government and regulatory agencies.
- Devise a disaster team training methodology and planning schedule.
- Have a plan that includes a schedule for routine maintenance and a list of "triggers" for maintenance reviews (such as an upgrade to desktop operating systems).

"The data for our live tickers used to flow into one data center. Now it flows into all three," Parker says.

He says the company's focus is to get everything in writing and form a cohesive back-up and recovery plan that is identical at every data center. "And now we are considering network switching, data routing, replicating domain controllers, equipment needs, electricity and efficient means to restore backup," Parker says. The plan is expected to take six months to complete.

Experts say disaster-recovery plans should evaluate the need for, or the configuration of, replication, redundancy clusters, software change management, remote access, access to back-up tapes or servers, and hot or cold sites. Companies also should establish "quick ship" programs from vendors for product replacement.

Plans also should include remote management in case of biological attack.

"If your site is evacuated, can you manage from a remote site if you can't get to your servers? That takes planning to assure, for instance, that your servers can be booted remotely," Gartner's Scott says.

Testing, testing

Kodak's Corcoran says that without testing you don't have a plan. "At a minimum you have to test once a year for critical applications and infrastructure. Our ERP recovery plan is tested three times a year," he says.

Corcoran says testing must be conducted only in a plan's established recovery center. "That sticky note on the server is of no help at that point," he says.

Chris Leach, national director of technology risk management for Grant Thornton, a global accounting firm, agrees that it is all about testing. "It's sobering when you run your first test and see what you missed. I have never seen a test that did not involve surprises," he says.

He says companies are now asking if backup is enough and if they are doing it right. "We ask them in response, 'Can you pull out your IT department and have it run somewhere else?'" he says.

Cost vs. risk

However, the extent of many organizations' recovery plans eventually will boil down to costs, which can be hard to determine.

Experts say spending can start at \$20,000 and go through the roof from there.

Corcoran says cost is hard to quantify because effective continuity planning has to be second nature.

"Any good corporate business continuity plan should be part of the culture," he says. "When you do something in the corporation you have to ask what it changes, if it increases risks. Continuity planning has to be part of the business process model."

But Gartner's Scott says there are low-cost steps that can be taken immediately.

"You can put together a crisis management team that puts flashlights in desks, [and] maintains call lists of personal phone numbers and e-mail addresses," she says.

Teplitsky, the network administrator at the Northeast telephone company who views those costs against the backdrop that used to feature the World Trade Center towers, says his company is considering spending \$400,000 just to install redundant storage that would replicate data daily.

Overall, he estimates the company could spend more than \$1 million just to ensure up-to-the-day data restoration. And that figure doesn't take into account ongoing maintenance and testing or other parts of the continuity plan.

Restoration Hardware



AUTOMATED UNATTENDED BACKUP




www.qualstar.com/146915.htm

[Qualstar](http://www.qualstar.com/146915.htm)

However, it is those kinds of figures corporate executives will wrestle with in trying to determine how much risk they can endure. ■

Security takes center stage

• BY SHARON GAUDIN

Doors that were usually left open before Sept. 11 at Precise Software in Dallas are now locked. Workers are quick to report anything suspicious - either in the building itself or online. And when something is reported, the company is a lot quicker to respond.

Precise Software may not have doubled its security budget or locked down its network since terrorist attacks ripped into the World Trade Center, but employees are on a heightened state of alert.

"I guess we have added to the security staff," says Kurt Ziegler, executive vice president of the \$50 million performance software company. "Now, everyone is on the security staff. Now everyone is involved, and that's good."

Corporate users and industry watchers say IT executives are well aware of the threat from conventional and cyber terrorism. The Sept. 11 attacks, and the devastation that so many companies faced, sent IT staffs across the country running to double-check their back-up tapes and put in nervous calls to their hot-swap sites.

What Sept. 11 fears haven't done, at least yet, is cause CEOs and executive committees to recalculate and expand their security budgets. In this time of economic belt-tightening, even the fear of a corporate attack hasn't made extra monies flow.

On the other hand, security budgets are being kept intact while other areas are being cut.

In many cases, enhanced security already was in the works. And users interviewed say there's no plans to curtail those expenditures.

"What we're seeing is that security accountability has shifted from the IS staff to the CEO," says Elad Yoran, executive vice president of RipTech, a network security firm in Alexandria, Va.

"Security now is a strategic issue rather than a tactical issue. Woe is the CEO who hasn't taken the measures to protect the company," he adds.

Yoran says client calls dropped to nearly nothing in the two weeks after Sept. 11 and then immediately spiked back up early in October to rates much higher than before the attacks.

Dave Jarrell, computer security officer at the Federal Communications Commission in Washington, D.C., says the terrorist attacks forced the agency to be more vigilant, both in monitoring its network and in keeping upper management informed about their efforts.

"We've always been very aggressive about system monitoring and having a proactive approach to computer security," says Jarrell, who monitors the perimeter of the network and traffic on the inside. "We're just a little bit more aware of what's going on... The entire population that focuses on security, whether cyber or physical, is more concerned about their programs."

And Jarrell says he used to report on security issues to his bosses as they occurred but now he makes weekly reports regardless of what is happening on the system.

"They have the assurance that on the cyber side of the house, everything is more attended to," Jarrell says. "There's more communication. It's more fluid now... If nothing has happened, I let them know that so they have peace of mind."

That peace of mind - or lack of it, actually - is most of the problem, according to some analysts and users.

Most major companies have been aware for years of the potential of a large-scale, coordinated attack on corporate America. But now those concerns, which were in the back of people's minds, are in the forefront of their security thoughts... and those fears come with visuals, thanks to the images of the attacks that were played repeatedly on 24-hour news stations.

"There's more of an awareness of what could happen," says David Smith, network manager of C&S Wholesale Grocers, a \$9 billion company in Brattleboro, Vt. "It's that knowledge of one's mortality... It makes it all seem more critical."

That feeling of vulnerability - both at home and in the workplace - has users testing the security measures they've already had in place, according to Daniel Woolley, COO of NetSec, a security company in Herndon, Va. Woolley says NetSec has seen a three- to fourfold increase in customers asking for vulnerability assessments. And he says for the first time, nearly every client calling in wants to know if NetSec's people have gone through security checks.

At First American Bank in Illinois, a \$1.6 billion financial institution with 32 branches, checking its own security strategy in light of the Sept. 11 attacks means creating a plan to split up the company's IT team.

"Since Sept. 11, the issue of the geographical dispersion of our staff really heightened," says Noel Levasseur, executive vice president of IT at First American Bank. "All of our IT department is in one location. If we had something catastrophic... we might have systems running but no one to run them."

The Infrastructure that Supports the Infrastructure White Paper

In this CRM Magazine white paper and case studies, find out how leading businesses are turning their disaster recovery strategies into important revenue-generating engines for their companies.

EMC²
where information lives

[>> view white paper](#)

[EMC² - Where Information Lives](#)

Levasseur says he now needs to figure out how to split up his IT team, whose members are used to working together. "I don't think it makes it more difficult to work but it makes the management challenging and the teamwork challenging," he says. "You can't always leave someone at a remote location. You need to rotate it."

Ziegler of Precise Software says it's important to make sure that changes in security strategy are changes with which workers can live - and work.

"People are much more amenable to security," Ziegler says.

"Before, it was a bother. Now they see the need. When someone puts rules in place, they're not complaining about it. . . . This is a good thing. It hasn't affected business. It's not intrusive and offensive," he adds. ■

How ready are the nation's networks?

• BY DENISE PAPPALARDO AND CAROLYN DUFFY MARSAN
(Senior Writer Michael Martin contributed to this story)

Disaster preparedness isn't new for carriers and ISPs, which have had to guard against earthquakes, floods and hurricanes since networks began crisscrossing the country.

But no one had planned - at least not fully - for the disaster that hit the U.S. on Sept. 11.

Most national network service providers were affected when terrorists attacked the U.S. Most claim their network readiness prevented a national tragedy from also becoming a technical catastrophe. However, a heightened vigilance has emerged since.

Experts agree that the Internet performed better than the circuit-switched telephone network during the attacks, but that's because the two networks are designed differently.

The U.S. military designed the Internet to route around structural problems like those occurring in Verizon's main switching facility in New York.

But when an entire central office switch site that serves thousands of customers is annihilated, it takes time to reroute calls to a different switching facility.

Verizon's West Street central office switch facility, which sits directly across from where World Trade Center Building 7 stood, was severely damaged. This site, which connected 200,000 voice lines and 3 million specialized private data lines, was pretty much out of commission. But with engineers at Ground Zero, Verizon had back-up switches and power supplies on the sidewalks in front of its West Street facility to get customers back online.

An unknown number of users were knocked off the Internet because several ISPs had points of presence in the World Trade Center. However, the Internet's distributed nature let most users maintain access.

Genuity lost a point of presence (POP) in the World Trade Center. While it took time for the ISP to get customers back online, Genuity says it

couldn't have done it without the help of Verizon.

ISP dependency on local networks is considered a vulnerability of the Internet, but it's a necessary evil.

Users who accessed Genuity's POP in the World Trade Center were looking to reconnect to the Internet from different sites around New York City and elsewhere. Genuity brought all of its customers back online in a matter of days, says Chris Yetman, vice president of technical support at the ISP.

While all of the service providers interviewed for this story had disaster-recovery and redundancy plans built into their operations before Sept. 11, all agree there is room for improvement.

This event triggered Genuity to examine its data centers and POP locations to ensure these facilities have broadband connectivity that guarantees redundancy.

"In the past we would allow a data center to be homed to the same POP on our backbone if it made the most sense from a network efficiency perspective," Yetman says. "We didn't think it affected redundancy because we weren't thinking about losing a whole data center. We thought about routers going offline or a backhoe chewing up a fiber line."

"It didn't take much to map things differently," he says.

Genuity redirected OC-48 connections from its data centers and POPs to different routers on its network for redundancy's sake. If Genuity lost a facility to a bombing today, traffic would be automatically rerouted.

Genuity has also taken steps to ensure that "certain high-profile customers such as government agencies" are easily and quickly identified and serviced in the case of an emergency. These government customers typically need additional circuits when a disaster strikes, but Genuity also has to ensure circuits aren't taken away from emergency relief efforts at hospitals or Red Cross facilities. Genuity has developed a plan to better locate and contact these customers when disaster strikes, a plan it did not have previously in place.

And while the ISP's network operations center (NOC) - essentially the heart of Genuity's backbone - has a back-up facility that could replicate

availability.com offers a broad range of topics that will help you:

- ▶ Recover from downtime disaster
- ▶ Improve service levels
- ▶ Reduce planned & unplanned downtime
- ▶ Conduct a downtime cost analysis
- ▶ Understand industry benchmarks & standards

Register Today and Receive FREE Gartner Research

availability.com
IT starts here

Availability.com

all monitoring, this site is only 12 miles away. The main NOC is in Woburn, Mass., and the backup is in nearby Burlington, Mass. The ISP also has a back-up facility in Columbia, Md., but this site is not as robust as the one in Burlington.

"We're aware of how close they are, and we're examining ways to lessen that vulnerability," Yetman says.

While redundant ISP networks play a key role in the reliability of the Internet, the fact that this is a network based on hundreds of private and public traffic exchange points is also a key element of its resiliency. The 'Net was designed to withstand outages.

In the late 1990s there were stories written about how vulnerable WorldCom's Metropolitan Area Exchange (MAE) East was because it was housed in the basement of a parking garage. However, even if MAE East was knocked out, the Internet would survive, although users would likely notice a slowdown.

Neither WorldCom nor Sprint, which also operates an Internet network access point in New Jersey, would grant interviews for this story, citing security concerns.

But other providers that operate exchange points on the Internet talked about how operations were affected by the events of Sept. 11.

"We have facilities in New York. The one that was close to Ground Zero suffered some struggles such as power failures as well as carrier failures," says Ali Marashi, vice president of technical services at InterNap, which operates 37 "global service point" exchanges. "But we had another facility, which kept kicking right along.

"The recent tragedy shows that even the best systems can have some weaknesses," he says. "It's a wake-up call to operations centers to better ensure that their back-up plans work as advertised."

Equinix, which operates six exchanges on the Internet, says it hasn't had to make changes to its physical environment or operational procedures since Sept. 11 because security was already high.

"What has changed since Sept. 11 is that customers are focusing on three areas: geographic diversity, network diversity and contractual diversity," says Jay Adelson, CTO and founder at Equinix. "Our customers are really getting deep into their understanding of how networks are actually built so they can find out if Network A and Network B are actually riding on the same glass."

International service provider Equant understands the need for geographic diversity. Equant, which offers voice, data and Internet services around the world, has five NOCs, but it's in the process of consolidating those locations into three since its merger with Global One. Equant will maintain three NOCs, in Reston, Va., Paris and Singapore. While these NOCs run regional network monitoring, they each have the capability of running full backup for the other.

"Any other NOC can watch the other, which is part of the reason the locations follow the sun," says Jack Norris, director of customer service at Equant.

Equant has learned new lessons about network reliability since Sept. 11. The service provider lost connectivity to Canada after the attacks.

"One of the circuits we purchased to be diverse was routed through Wall Street," Norris says. That was a surprise because the circuit was to connect New York's Long Island to Toronto and Montreal.

"We didn't expect that particular facility would be in a different borough, and we didn't expect it to go through lower Manhattan. If we knew, we would have asked for a change," Norris says.

Equant has reexamined local connectivity for its networks. The service provider is committed to running more frequent audits to be sure local connectivity is in the best location.

Equant has also stepped up physical security at its NOCs and offices.

"There have been more advisories about travel to different countries, information about suspicious packages and building security," Norris says. Instead of leaving the front doors open with a security guard, Equant now has employees "badge in" at security boxes outside all doors.

AT&T also has beefed up security at its NOC in Bedminster, N.J.

"I was able to drive up to the gate and put my ID on a sensor and gain access to the grounds. Now I have to physically be let into the building," says Art Deacon, vice president of network operations.

AT&T has one back-up NOC, but says it has never publicly revealed this location. In addition to a fully redundant NOC, each network has its own operations center, Deacon says. Frame relay, ATM, private line, IP and voice each has its own mini-NOC.

Deacon says that on Sept. 11, AT&T's voice network performed exactly as it should by handling 431 million calls, considerably more than the typical volume of 330 million calls.

But because AT&T shared space at Verizon's West Street facility in lower Manhattan, it needed to deploy its disaster-recovery team to the site.

AT&T had its switching node, which is essentially a mobile central office voice switch deployed on two tractor trailers, in New York within 48 hours.

AT&T's typical disaster-recovery plan calls for engineers to fly into the disaster site from parts of the country that were not affected. That was more challenging in this case because flying was not an option. Deacon says staffers drove to New York from as far away as Jacksonville, Fla. Engineers manned the mobile facility, working 12-hour shifts, for six weeks.

"We spent \$300 million to have the ability to recover a switching facility," he says. "We have tractor trailers in four different geographic areas in the country that can be accessed from any point within the contiguous U.S. within 24 hours," he says.

Verizon, which suffered the bigger blow after the attacks, is making progress. The core of Verizon's network in downtown New York will end up in better shape than before the attack because many components are being upgraded. Asynchronous technology is being replaced by SONET. And many buildings, which formerly had copper connections, will now have fiber.

There also won't be as much reliance on the company's damaged West Street central office.

"We've had to increase the infrastructure in the other central offices with West Street down, and they will continue to take a heavier load in the future," says John Bell, senior vice president of network operations at Verizon.

Details of preparing for another catastrophe will differ from one carrier to the next, but the foundation of all plans appears to be common, experts say.

"One assumption that has absolutely changed," Equinix's Adelson says, "is the notion that you can build a data center so well that it can withstand anything." ■

Planning for the worst: Bring in the best

• BY KATHLEEN OHLSON

Thinking of overhauling your disaster-recovery plan? Fortunately, there are many companies that can give you some pointers.

The first step, of course, is acknowledging that disaster could affect you. "Never underestimate the human gift called denial," says Bruce Malik, an analyst at Gartner. "I think a lot of folks think they're luckier than average."

Next, recognize that there is a difference between business contingency and disaster recovery, and that plans for both are necessary. Business contingency means planning ahead for an emergency and identifying a plan to ensure critical networks and systems are up and running.

Disaster recovery, on the other hand, refers to a plan for reacting to an event.

Companies such as IBM Global Services' Business Continuity and Recovery Services, Comdisco and SunGard can help you formulate business contingency and disaster-recovery plans.

These organizations interview key personnel and evaluate network, system and recovery plans, if there are such plans. They then come back with recommendations.

When developing and implementing contingency and recovery plans, it's important to keep it simple, according to experts.

"Disaster-recovery planning is a complex task, but organizations make it more complicated by throwing everything but the kitchen sink into the plan," says Damian Walsh, Comdisco's senior vice president of professional services. The tendency is to spell out plans for everything - each unit, facility and employee, and "it becomes hundreds of pages," he says. "It's analysis paralysis."

Walsh says companies need to keep plans to one to two pages.

When an emergency occurs, consultants help companies restore operations by duplicating systems at a vendor's recovery site, shipping hardware replacements, moving operations and employees to hot sites, or bringing mobile centers to companies.

Build it in

By automating data recovery, it becomes one less matter to worry about when disaster strikes. "You have to figure the senior technical people won't be available [to recover data], and people who are available will be inexperienced or not mentally ready to do the job," says Rick Weaver, BMC Software's product manager for OS/390 recovery and storage management. "You forget the human element, so you automate as much as possible."

Network management tool vendors - including BMC, Tivoli Systems and Hewlett-Packard - offer a range of software that can back up and recover data on databases, monitor performance, recognize when new devices join a network, and manage who accesses certain information.

Industry analysts say that up to 60% of a company's critical data is stored on individual laptops and desktops. Network executives looking for more control over PCs can turn to companies such as Connected, which

Where to turn

Some of the organizations that specialize in business contingency and disaster recovery include:

- **American Red Cross**
www.redcross.org/services/disaster/beprepared/busi_industry.html
- **BMC Software**
www.bmc.com/products/rmds/index.html
www.bmc.com/products/rmos390/index.html
- **Comdisco** www.comdisco.com
- **Connected**
www.connected.com/products/index.htm
- **FEMA** www.fema.gov/library/bizindex.htm
- **Hewlett-Packard**
www.managementsoftware.hp.com/products/index.asp
- **IBM Business Continuity and Recovery Services**
www-1.ibm.com/services/continuity/recover1.nsf/documents/home
- **Institute for Business & Home Safety** www.ibhs.org/ibhs2/
- **Sanrise** www.sanrise.com
- **Storability** www.storability.com
- **StorageNetworks** www.storagenetworks.com
- **SunGard** www.recovery.sungard.com
- **Tivoli Systems**
www.tivoli.com/products/solutions/availability/
www.tivoli.com/products/solutions/security/
www.tivoli.com/products/solutions/storage/products.html

provides software for automated desktop backup and recovery to rebuild users' systems, right down to the wallpaper.

"Disaster recovery is a labor of love that needs to be nurtured, but it's everybody's stepchild," says Lou Berger, a StorageNetworks executive. "It's done begrudgingly and not often done well."

Some businesses are turning to storage service providers (SSP), such as Sanrise, Storability and StorageNetworks, for help. SSPs manage data storage for customers at their headquarters or collocate storage with other service providers in major cities, providing primary or secondary back-up storage.

Community organizations

Government and community organizations, such as the American Red Cross and the Federal Emergency Management Agency, help businesses when it comes to personnel issues during disasters.

Before a disaster strikes, they say businesses should find out about available resources from local community government liaisons; public, fire and police departments; telephone companies; and electric utilities.

Other recommendations include:

- * Compile a phone list of key employees and customers, and provide copies to staff members. Create emergency call lists - preferably wallet size - of all persons on- or off-site who would be involved in an emergency, their responsibilities and contact information.

- * Designate a phone number for recorded messages and provide that number to employees.

- * Meet with insurance companies and assess the potential property, business and human interest impact of a disaster.

- * Have building and site maps featuring the locations of utility shutoffs, gas lines, exits, stairways, designated escape routes, restricted areas and high-valued items.

In light of the terrorist attacks, many vendors have seen a dramatic increase in businesses seeking advice to revamp or create contingency and disaster-recovery plans.

"It's going to take a long time to forget those images, how it affected so many and the impact on businesses," BMC's Weaver says. Businesses are thinking about data protection beyond their own business, by expanding their supply, manufacturing and distribution contacts.

But StorageNetworks' Berger is skeptical about businesses' intentions for business contingency and disaster recovery.

"It'll likely wane in certain industries - and by December, you'll know who's serious about it when the budgets are made," he says. ■

Spending shifts

• BY NEAL WEINBERG

The events of Sept. 11 have caused many IT executives to shift their spending priorities in 2002 toward disaster recovery, security and videoconferencing, but the weak economy is having a far greater impact on IT budgets than the terrorist attacks.

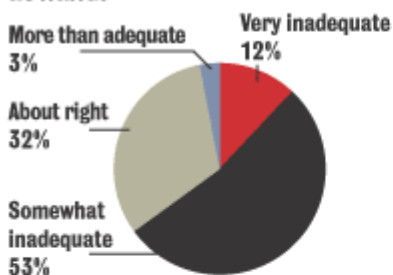
Those are some of the key findings from Network World's annual IT spending survey, which was expanded to include questions relating to the September attacks. A total of 598 IT professionals responded to the survey, which was conducted by Research Concepts of Berlin, Mass.

When it comes to overall spending for 2002, IT budgets appear to be inching up only 3.9%. That's a far cry from the 9.9% increase seen in 2001. Forty-two percent of this year's respondents say their 2002 spending is increasing, while 30% say their budgets will be flat and 28% are facing budget cuts.

Not surprisingly, only 35% of the IT professionals surveyed said that their 2002 budgets are adequate or more than adequate, while a sizeable

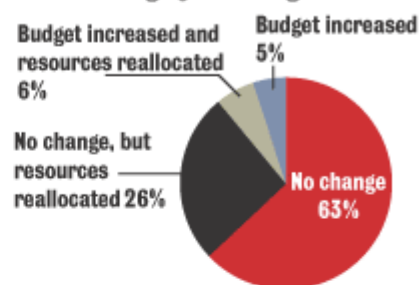
Feelings of inadequacy

How do you feel about the financial resources you have relative to the tasks at hand?



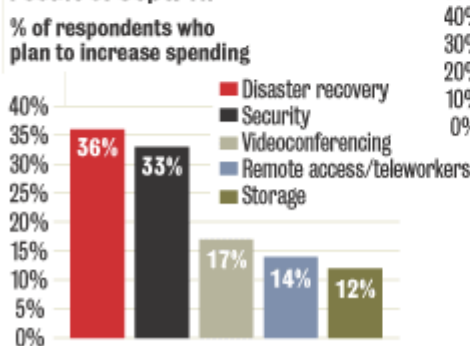
Most budgets unchanged

How did the events of Sept. 11 change your budget?



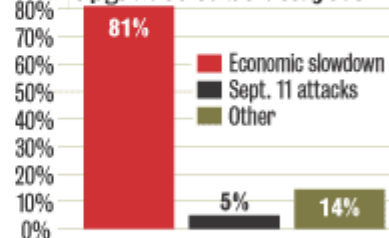
Impact of 9/11

Did you decide to increase spending in any area as a result of Sept. 11?



Upgrades delayed

Which factor caused upgrades to be delayed?



Budget-stretchers

What steps are you taking to stretch your budget?

1. Delay purchases
2. Consolidate servers
3. Renegotiate contracts
4. Manage remotely
5. Move functions to the Web

majority - 65% - stated that their 2002 financial resources will be inadequate to handle the tasks at hand.

When asked which specific areas will receive more money in 2002, the top answer by far was security, which was listed by 62% of the IT professionals surveyed. Disaster recovery was named by 45% of respondents, followed by storage, wireless, servers, remote access/teleworkers, network management tools and LAN infrastructure.

Then we asked about the impact that Sept. 11 had on spending. Thirty-six percent said they'll be spending more on disaster recovery because of the attacks, 33% said they'll increase security spending, 17% plan to boost videoconferencing and 14% are looking at increased remote access investments specifically because of the events of Sept. 11.

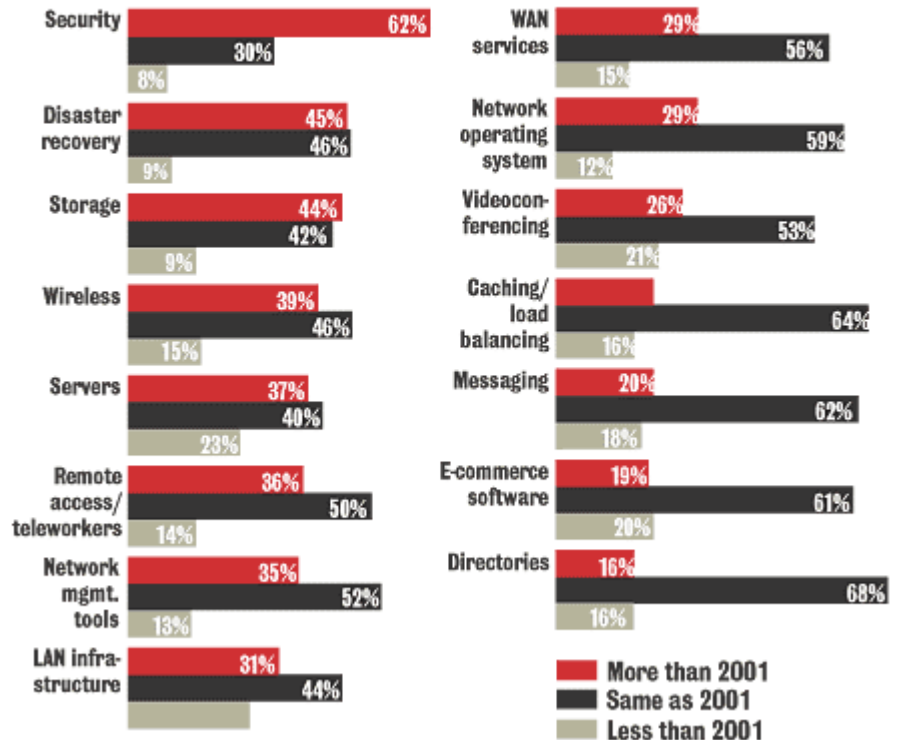
But only 11% of respondents said they will receive additional money as a result of the September attacks, while 63% said there is no change in their budget, and 26% are shifting resources within their budget to areas that have become high priorities.

Finally, nearly 30% of IT professionals had to delay a technology upgrade slated for 2002. The most common upgrades that are being put on the back burner are operating system upgrades, enterprise applications such as customer relationship management or enterprise resource planning, wireless and infrastructure or backbone upgrades.

But IT professionals, by an overwhelming margin, said the upgrade delays are due to the economic slowdown, not to any budget shifting caused by Sept. 11. ■

Spending priorities

How will spending in 2002 compare with last year in these specific areas?



Internet resource links for Disaster Recovery and Business Continuity

Network World news stories on disaster recovery and business continuity:

<http://www.nwfusion.com/topics/disaster.html>

[Disaster recovery glossary](#)

Disaster Recovery Journal.

[Business Recovery Over Wide Area Networks: Are You Ready?](#)

Article discusses the need for disaster recovery plans as well as tools available to assist. Free online registration required. Webtutorials.com.

Disaster recovery audio primer

Learn how to start the disaster recovery planning process, what needs to be included in a plan and some of the options available.

<http://www.nwfusion.com/primers/disaster/disasterprimer.html>

The Business Continuity Planners Association Web site

The BCPA, based in Minneapolis-St. Paul, is a non-profit, mutual benefit association of business professionals responsible for, or participating in, business recovery, crisis management, emergency management, contingency planning, disaster preparedness planning, or a related professional vocation.

<http://www.bcpa.org>

Infosyssec – Security Portal for Information System Security Professionals Web site. Large number of resources specifically related to Business Continuity and Disaster Recovery Planning

<http://www.infosyssec.com/infosyssec/buscon1.htm>