THE CHRONICLE
of Higher Education

Technology

February 28, 2003

Preparing for Computer Disasters

By DAN CARNEVALE

Advance planning and backup systems allow colleges to recover data

Marc F. Elvy prepares for disasters, but he wasn't prepared for what he saw when he showed up at work one day in December.

The University of Washington's Educational Outreach office, where Mr. Elvy is the network manager, was on fire. For eight hours the top floor of the two-story building burned while the fire department trained hoses on the flames.

After the fire was extinguished, another seven hours passed before Mr. Elvy could persuade the fire marshals to let him into the building. He found just about everything on the second floor, including the computers, either melted or burned to a crisp. A foot of water flooded the first floor, where the office's 17 main computer servers were housed.

"The whole ceiling came down on the first floor," Mr. Elvy says. "It was just a soggy, pasty mess."

Mr. Elvy fished some of the waterlogged servers out and loaded them into his pickup. He also found some software disks floating in a briefcase in the building. Then he drove home and spent the next several days working with a space heater and his wife's hair dryer.

He was able to save some of the e-mail data the servers contained. But most of the 17 machines were useless, and many of them held student records and registration information for the university's online courses.

Fortunately, the university saves all important computer data every night on tapes that it keeps off the campus. The university also has a supply of spare servers for emergencies. Mr. Elvy and his staff members had the educational-outreach network and its online services back up and running after just one business day, although at a slower-than-normal pace. It took two weeks of work, over the Christmas holidays, to bring everything up to full speed.

But for every story of how an institution was able to save its data, a professor somewhere has a horror story about losing years of research after a fire, natural disaster, or a server crash. And while most large universities religiously back up their main computer servers every night, some only save data on smaller servers once a week. And faculty members may or may not back up information they save on their own machines. Such information, sometimes including grades and research, is often at risk of being lost.

Most colleges have some sort of plan to protect their computer information, although few have faced the kind of disaster that would demonstrate whether those plans actually worked. Experts say staging a mock computer disaster can highlight a preparedness plan's shortcomings, but such tests happen only rarely.

Some smaller institutions, meanwhile, can't afford extensive backup systems, which can cost hundreds of thousands of dollars. Because of the expense, some institutions don't buy backup computer systems at all, or do much to protect the data in their servers.

Backing up computer data for critical functions, like payroll and personnel files, is a common business practice. The attacks on September 11, 2001, and the constant threat of terrorism have helped push the issue of disaster preparedness.

A faulty fluorescent light caused the fire at the University of Washington's Educational Outreach office. The building, which the university rented from a private landlord, was old enough that a grandfather clause exempted it from automatic-sprinkler requirements. Luckily the building was unoccupied at the time of the fire.

The blaze caused about $1-million in damage. Insurance will cover most of the expense, including the $170,000 cost of replacing the computers.

David P. Szatmary, the university's vice provost for educational outreach, says he had never paid much attention to the backup systems until the day of the fire. "The first fear when I saw the flames was, 'I hope that our data was backed up,'" he says.

Even though almost all the information was saved, staff members discovered that "working from backup tapes isn't the easiest thing in the world," Mr. Szatmary says. The staff worked many late nights transferring information to the backup servers, which was a challenge in its own right: A system that had worked on 17 servers now had to be handled by 3, meaning that response times were slower for users.

Mr. Elvy says the cost of having the spare servers ready to use was $5,000 each, and that tapes for the regular backups cost $14 apiece (staff members handled the chore as part of their regular duties). When all was said and done, it was money well spent, he says. "As

far as my position goes, this is what I plan for, even though I hope it doesn't happen," Mr. Elvy says.

Fire Claims

The fire at the outreach office wasn't the first disaster to strike the University of Washington. In May 2001, the Center for Urban Horticulture was set afire. No one was arrested for the act, but a radical environmental group called the Earth Liberation Front took credit for the blaze. Members of the group claimed in a statement that they were trying to destroy genetic research being conducted in the center's labs.

In that fire, many faculty members lost their research materials, some of it on hard drives and some on paper or in artifacts. While the professors who work at the horticulture center can back up all their data on the university's servers, many hadn't taken the time to do it. Others had backed up their data on disks but left them in their desks, which burned in the fire.

Thomas M. Hinckley, director of the Center for Urban Horticulture, had important information on his hard drive, including historical data on Mount Saint Helens and digitized images of other research. The university paid a company $2,500 to recover as much of the information as possible, but about a quarter of it was beyond recovery. It has taken Mr. Hinckley a while to figure out just what data he has lost. "It's one of those things -- as time goes by you look for old files and you can't find them," he says.

Other faculty and staff members' computers required similar attention to save data that were not backed up. "It's lazy -- you're working up to the last minute of the day, and instead of taking 10

minutes to save things, you just assume everything will be OK tomorrow," Mr. Hinckley says.

The one person who didn't lose any data was Toby Bradshaw, a professor in the departments of botany and zoology whose work was the target of the attack. The vandals set fire to a five-gallon drum of gasoline in his office to destroy his research on tree genetics. But he had backup copies of everything off-site.

Learning From Experience

Observers say that most universities are doing at least the minimum necessary to protect computer data, although college officials tend to think more along the lines of server crashes than widespread disasters. And while many institutions have plans that protect data, few have well-thought-out systems for recovery once a disaster has happened.

Jon W. Toigo, chief executive officer of the consulting and analysis company Toigo Partners International, says data recovery often isn't a big priority for an institution unless people there have already witnessed some major catastrophe.

"That's usually the motivator, that they've experienced a disaster, and they're trying to prevent it from happening again in the future," Mr. Toigo says. "You really have to think about recoverability before you build the system."

At the very least, he says, colleges should have some sort of procedure for automatically saving the data. "As long you've got the data backed up, you can buy another system from CompUSA," Mr. Toigo says.

Cole Emerson, chairman of the Disaster Recovery Institute International, which teaches organizations how to protect data, says every business and institution should do at least three things to protect data. First, he says, back up the data. Second, store the backed-up information off-site. Third, have contact information available for people who can help retrieve the information at a moment's notice.

While those are the minimum recommendations, institutions would be wise to also have extra servers on hand so data can be retrieved immediately and services can be restored quickly. And officials should have extra copies of software available to retrieve the stored data.

A Daunting Task

Just 90 miles north of the University of Washington is Western Washington University, which had its own scare in July when the room containing the computer nerve center for the College of Business and Economics was destroyed by fire. The data were backed up and copies were kept off campus. But the officials found the task of putting the pieces back together more daunting than they had expected.

Dennis R. Murphy, dean of the college, says the data were backed up in preparation for a server crash, not necessarily a widespread disaster. "Fire was rather far from our radar screen because this building is brick, so there's not much to burn," he says.

The university had spent over $100,000 on backup servers, and that saved both time and money, Mr. Murphy says. But he says officials had never tested their ability to retrieve backed-up data using other people's equipment. It took a couple of weeks to recover all the

information, and the university had to spend a couple of hundred dollars for each computer that needed to be decontaminated. The cleaning bill alone was in the thousands.

Student records and other critical data were saved. But some faculty members lost research data. "There's a lot more individual backing up going on now," Mr. Murphy says.

The computer room in the building has been rebuilt, and now it has a smoke detector installed. And business-college officials have assembled a CD-ROM that contains emergency information, such as a vendor contact list, student-identification information, and a record of the last payroll run. Each administrator gets a copy of the CD, which is updated monthly, so he or she can dig up important information during the first 24 hours after a disaster.

"A lot of places take care of the big things," says Jerry Boles, Western Washington's vice provost for information and telecommunications services. "But it's these little things that can be very frustrating."

The only way to identify those little things is by doing practice drills, Mr. Murphy says. "You need to do dry runs," he says. "It's a pain in the neck, but it's the only way to find out."

Paul Ellis, program director for IBM Tivoli storage management, says drills should be conducted a couple of times a year. Tivoli is a branch of IBM that sells services and equipment for protecting computer data to businesses and institutions.

During those drills, he says, officials will be able to tell whether the stored data are easily accessible and compatible with other

equipment. Drills also make people realize that they need spare copies of the software to run the data they've been storing.

"The scary part is if you're planning for this disaster, and it fails in the calm moment, what's going to happen in a real disaster?" Mr. Ellis says. "Everybody talks about backup, but the really important part is how long it takes to do a restore."

Although larger universities find it is worth their while to develop elaborate backup systems, community colleges don't always have the cash on hand to make that sort of investment.

John R. Moore, associate dean of computing services at Allegany College of Maryland, says the two-year college can't afford to put much money into backup systems. So officials there make do with what they can. "We looked into buying disaster-recovery capability, and it was rather expensive," he says.

Instead of using an automated backup system, staff members manually save information on tapes. Instead of keeping backed-up information off site every night, staff members put the tapes in a fireproof vault in the same building as the computer servers.

Once a week, the tapes are taken to an off-campus location. While the fireproof vault offers some protection, the heat from a fire could make the data on the sensitive computer tapes unreadable. And if the building collapses, it could be weeks before the data could be retrieved. But that's the best that Allegany, a college with 3,000 students, can do, Mr. Moore says.

Spending Varies Widely

Allegany has not had any problems so far with its system. But if a fire did knock out the computer servers, Mr. Moore says it would

take two to four weeks to acquire new equipment. Classes could continue, he says, unless they were conducted online.

Not all community colleges have to scrimp when it comes to creating a backup system. The Community College of Baltimore County has off-site backup systems, and the college hasn't lost any data despite two incidents in which networks were damaged by water leaks, says Wally Knapp, director of information technology and technical services there. He says he doesn't know how much the college spends on backing up the data, but it's well worth it if it means a good night's sleep for everyone involved.

Other institutions have had close calls that have compelled them to take broader precautions. In 1998, the University of Missouri at Columbia was struck by a minor tornado that tore the roofs off some campus buildings. No data were lost in the incident. But Willie Jones, records analyst at the university, realized that its computer records weren't protected well enough.

So the university created a mirror site, complete with computers and duplication of most crucial data, five miles away. The university would not reveal the cost of the operation for security reasons.

Some universities save money by finding ways to make their backup systems productive long before disaster strikes. Instead of having backup servers sitting around doing nothing while they wait for a disaster, Northwestern University uses the equipment for low-priority tasks.

"They may be e-mail servers in a normal situation, but they may end up doing payroll if that's what we need" in a crisis, says Mort Rahimi, vice president and chief technology officer at Northwestern.

The university invested $300,000 in backup servers and spends about $5,000 a month storing data on backup tapes. Critical information is saved every night while other information, such as research data, is backed up weekly. It's up to faculty members to decide whether to save their data on university servers instead of on their desktop machines.

"The big risk, of course, is if somebody has been working on something for years. If a disaster strikes, they'd lose that data," Mr. Rahimi says.

As Mr. Hinckley at the University of Washington can attest, it's worth the extra effort to save research information on the university servers. "My view is, you back everything up," he says. If there is a fire, you don't lose anything, he says, and "you get a new computer out of it."

---

http://chronicle.com Section: Information Technology Volume 49, Issue 25, Page A33