Preparing for IT Disasters

PRINT | EMAIL

🔲 DIGG THIS
🔲 SAVE TO DEL.ICIO.US
🔲 SEED NEWSVINE

School districts need a step-by-step plan to create a safety net.

Karen D. Schwartz

Earthquakes. Floods. Even threatened terrorist attacks. Any of these disasters can quickly bring a school district to its knees, preventing it from accessing mission-critical data and systems.

The best way to prepare for an information technology disaster of any type is by being proactive — assessing your needs and weak spots and developing a step-by-step plan to mitigate both natural and man-made disasters that might affect your critical IT.

Tony Korwin certainly learned that lesson the hard way. On his third day as director of technology for Alamogordo (N.M.) Public Schools, Korwin experienced what some might call a baptism by fire. A citywide electrical brownout caused the school system's mainframe to lose three of its 35 drives that contained crucial financial, human resource and student information.

A brownout during Tony Korwin's first week at Alamogordo (N.M.) Public Schools caused him to quickly revamp the district's data backup plan.

Photo Credit: DOUG MERRIAM

After paying $20,000 in overtime to employees who re-entered much of the lost data, the school board directed Korwin to do whatever it took to make sure a disaster never again compromised valuable school district data.

Korwin immediately installed a battery backup surge-protection system for the school district's server farm and worked to improve the district's data backup plans. He also developed a strategy for replacing any outdated equipment.

Korwin and his staff then switched into high gear and developed a full-fledged disaster-recovery plan that covers every possible parameter: hardware and software standards, the priority level of various data, equipment redundancy, educating users on roles and responsibilities, and handling outside attacks and viruses. Their strategy includes developing a plan for use in case of a pandemic, creating a physical location for off-site restoration, handling Internet service provider downtime and educating the staff on how to develop a three- to five-day downtime plan.

Backing Up on a Budget

Brian J. Dooley, an analyst with more than 20 years of experience examining IT trends, recognizes the important role data plays in today's schools, but realizes that money remains tight for public education. He has created a budget-based plan that allows schools to protect vital information without spending a fortune.

Schools can optimize the recovery process by prioritizing what needs to be stored, determining the profile of data that must be restored (i.e. how much, how recent and so on), and cataloging potential risks and the likelihood of occurrence, he writes in the 2006 report, "Disaster Recovery on a Budget," from Info-Tech, a research group in London, Ontario. One of the best ways to protect data in many types of situations is to have the information stored in separate locations, he says.

School districts can outsource this work to vendors specializing in recovery. This can allow a district to tap into state-

Hurricane Warnings
The U.S. locations with the highest probability for hurricane strikes:

- Miami 48%
- Cape Hatteras, N.C. 48%
- San Juan, P.R. 42%
- New Orleans 40%

Source: National Oceanic and Atmospheric Administration

of-the-art equipment and methods without making any capital expenditures. No matter what plan a school district takes, officials must keep it up-to-date, he says.

Slow but Steady Progress

Montgomery County Public Schools in Maryland has been proactive with its disaster-recovery plan, developed about five years ago. The first step, says John Q. Porter, deputy superintendent for information and organizational systems, was developing a vision, with information availability as the centerpiece.

To gather information, Porter's team engaged a number of internal stakeholders, including senior administrators at the central office, teachers, database and network administrators, software applications staff and the chief security officer.

"The key was how to attain high availability of all systems and information. First we defined what we considered to be a disaster — when our data center was unavailable due to an unplanned event for more than 72 hours and impacted the entire district," Porter says.

Next, the team performed a business-impact analysis, listing everything that should be recovered. "The most important thing for us was our mission-critical systems and applications that were essential for meeting educational requirements, such as HR and payroll," he says.

Broward County, Fla., has gone a step further, turning to technology to combat communication mishaps. "After the five hurricanes we've been through [in] the last five years, the fear was we might have a complete breakdown with no communication," says Jerry Graziose, director of safety for the county's Educational Technology Services.

So the county outfitted a trailer with satellite connections that would house a generator, and through the satellite would have limited communications with the Department of Education or other agencies in an emergency.

The county also has a backup location, or hot site, in Philadelphia, where employees could recover critical applications such as the student records, payroll and financial systems.

Crucial to being prepared to resume operations at a remote location is adequate testing and training, says John Alawneh, executive director of technology operations for Plano (Texas) Independent School District. "Our people go through special training to make sure they can restore systems in a timely fashion and switch to and from hot sites," he says.

No matter what approach an organization takes toward shoring up its IT infrastructure in preparation for a disaster, it's essential to do something and leave as little to chance as possible, New Mexico's Korwin says.

In the final analysis, he says, "We figure that it's better to have an imperfect plan implemented than a perfect plan unimplemented."

Mitigating the effects of a disaster

While no technology exists to prevent an IT disaster, a fully developed, fully tested disaster-recovery plan can help mitigate the risks. Here are some tips from school district IT managers:

- Before developing a plan, conduct a risk assessment to understand the business of the organization, including what data and systems are most valuable.
- Know your strengths and weaknesses. Hire experts to validate where you are on target and where you have vulnerabilities.
- Practice and test the plan regularly, as if a disaster were taking place.
- Create an incident-management team consisting of executive management and department heads, which will manage communication, direct response and recovery activities, monitor the recovery process, and provide or reallocate recovery resources.
- More than technology, adequate communication is the key to success.
- Revisit your disaster-recovery plan every year or two to address district-wide technology and other changes. — Karen D. Schwartz

Climatic Events

With the number of natural disasters the United States has experienced over the past century, it's no wonder school districts are taking steps to ensure the safety of their assets.

- An average of three major hurricanes cross the U.S. coast every five years.
- In 27 years, the U.S. mainland has gone two years without a hurricane twice: 1981–82 and 2000-–01.
- Flash floods often bring walls of water 10 to 20 feet high.

- The average forward speed of a tornado is 30 mph, but may vary from stationary to 70 mph.
- Peak tornado season in the southern states is March through May; in the northern states, it is late spring through early summer. Hurricane season stretches from June 1 through Nov. 1.

Sources: U.S. Geological Survey, National Hurricane Center, Federal emergency management agency and Noaa