

Disaster recovery



BY DAVE MILLAR

Imagine this scenario: A graduate student running a computer system for his lab's sponsored research project is unable to start the system one morning. A service technician diagnoses the problem as a "head crash"; the hard disk has been physically damaged. No data can be recovered, including the project research database, representing several years of work. Backup copies had never been made.

Qué será será?

Disasters caused by fires, floods, or hurricanes are rare and never touch the lives of most people. But a burst pipe, a hard disk failure, or the accidental slip of a finger onto the "delete" key are much more likely, and can have devastating effects. If you're a faculty member, could your research survive the loss of your data? Could you continue classes without access to your teaching materials, grade records, or classrooms? If you're a student, could you recover your classwork—papers, problem sets, projects? If you're a staff member, could you continue to provide critical services to the University following a disaster? You can take steps to minimize the impact of a disaster. By developing a disaster recovery plan, you can increase the likelihood that you will be able to perform critical tasks. The three elements to a disaster recovery plan—the risk management plan, the emergency response plan, and the business continuity plan—are described below.

Risk management plan

The risk management plan identifies how you will protect the key resources on which you rely.

If you rely heavily on paper files, consider:

- Use of off-site archival storage (The University Records Center provides secure storage for University records. For details, see the green pages of the Penn telephone directory.)
- Purchase of a fireproof vault or cabinet to protect documents
- Use of microfilm/fiche or imaging to copy irreplaceable documents

If you rely on computer data, be sure that your data is backed up. As Penn's computing environment becomes more distributed, responsibility for the integrity of institutional data that may reside on personal computers or workstations becomes distributed as well. In order to ensure the integrity of distributed data residing on personal computers or workstations, individual computer users must assume primary responsibility for taking adequate precautions against loss of their data.

Whether you provide your own computing capability or rely on others for that service, make sure that backups of your files are kept, and that they meet your needs. Make sure that files are backed up frequently enough, that no critical files are omitted, and that backups are kept in secure locations separate from where the original files are stored.

Penn offers PennBack, a PennNet-based backup service. PennBack provides a way to automatically schedule your backups over the campus network. Platforms supported include Macintosh; IBM PC/compatibles

running DOS, OS/2, and Windows; Sun; RS/6000; Novell NetWare; Hewlett-Packard HP-UX; DEC ULTRIX; and SCO UNIX. For further information about PennBack, contact Michael Kearney (michael@udcmail).

Also, be sure that your computing equipment is protected from problems with utilities, such as power surges and power failures. Larger equipment may need protection from a possible loss of chilled water for cooling. Information Systems and Computing (ISC) provides skilled system management and backups, and will house your computing equipment in a climate-controlled, power-conditioned environment.

Emergency response plan

The emergency response plan documents critical information you will need in the immediate period following a disaster. Copies of the plan should be kept away from the office (at home, in cars, etc.). Parts of the plan should be communicated to those who rely on you or your group so they can reach you in an emergency. This plan might include the home phone, address, beeper, and cellular phone numbers for key individuals, such as team members, other departments who rely on you, major Penn service providers, outside vendors, etc.

The most important thing about the emergency response plan is that it be up-to-date. It should be updated at least annually.

Business continuity plan

The business continuity plan states how an organization will provide critical business functions following a disaster.

When developing the business continuity plan, don't try to ensure that all functions will continue. Concentrate on critical functions and the resources you'd need to perform them.

Plan for the worst-case scenario. Six to eight weeks sounds like a long time to be without computing capability, but imagine how long it would take to acquire replacement computer equipment, software, and data—especially if your organization runs a large computer or a local area network.

Imagine you are denied access to your office, or that the computer you use is unavailable. How would you carry on business? Could it be done manually? Are there places on campus where you could get critical information? Are there organizations you rely on for critical services who may be similarly crippled (e.g., campus mail, telephones, PennNet, UMIS, Registrar)? If so, contact them and determine their capabilities so you'll know what to expect and what to plan for. Make a list of critical resources you'll need to obtain on an emergency basis (hardware, modems, software packages (including version numbers), fax machines, etc.). If you discover it's not

feasible to maintain certain critical functions, notify those who rely on them so they will not be caught off guard.

Next steps

Once you have developed your plan, don't let it gather dust. It is important to review the plan annually. Check the phone numbers in the emergency response plan to be sure they are up to date. Consider whether there are any new critical functions that your department has taken on which need to be provided for in the business continuity plan.

It is also important to test your plan. Periodically try to restore a file from your backups. One way to test your business continuity plan is to review it with the people who do the work to see if they think it will work.

Essentially, disaster recovery planning is a process of thinking through in an orderly fashion what you would be forced to think through frantically should disaster ever strike. The chances are you'll never need it, but taking time now could pay off in the future. If you would like assistance in developing a disaster recovery plan for your department, or for further information about services described in this article, contact Dave Millar at security@isc.

Note: Incidentally, there may be hope for the unfortunate grad student with the crashed hard disk. Search PennInfo, (keyword "data recovery") for further information.

DAVE MILLAR is University Information Security Officer.

Office of the Comptroller

Comptroller's Office staff developed a disaster recovery plan this year, following an analysis of Penn's disaster readiness by Dataguard Recovery Services of Louisville, Kentucky. Each department within Comptroller's planned how it would provide critical functions to the rest of the University following a disaster. An emergency response coordinator was appointed to maintain the plan and ensure continued employee awareness.

Dataguard surveyed most departments at Penn and assessed their preparedness. If you want a copy of the report for your department, contact the information services provider for your group or Dave Millar at security@isc.