Human Aspects of Computing

Henry Ledgard Editor

Disaster Recovery Planning For Academic Computing Centers

Planning for recovery from a disaster is quickly becoming recognized as a necessity for higher education computing installations. This article presents a structural framework, describes the stages, and tells how to implement a disaster recovery plan specifically geared to an academic computing organization.

Renate Rohde and Jim Haskett

Disaster recovery planning is a topic receiving increasing attention in recent issues of computer-related publications. Growing numbers of organizations are becoming aware of the need for such planning, but admit they have taken little action as a result of that awareness.

Thus, the necessity for a disaster recovery plan is currently making its way into the consciousness of computing facilities at educational institutions. The developers of a disaster recovery plan in an academic setting, however, are faced with obstacles above and beyond those confronting developers in a more business-oriented setting. Most of the literature on the topic is not directed at an academic environment and thus the concepts are hard to transfer. In contrast to businesses, which often run a limited number of applications and have a limited set of users, academic computing centers are generally service organizations serving thousands of users, each running different applications. Academic institutions are typically not-for-profit organizations having limited resources with which to develop and implement a plan. Furthermore, they cannot calculate the cost of failing to offer service and thus cannot justify the cost of disaster recovery planning. These factors combine to make it particularly difficult to develop a disaster recovery plan in an educational environment.

Therefore, the purpose of this article is to provide the conceptual outline for a disaster recovery plan specifically geared toward an academic setting, and to provide some concrete examples from a plan we created at a large midwestern university of 35,000 students. The academic computing environment consisted of a large CDC mainframe, an IBM mainframe, three PRIMEs, and nine VAXs. The facilities consisted of a single large building which housed the machine room and offices for approximately 75 staff members, a number of remote public terminal and PC clusters, and their related networks.

Creating a Plan in an Academic Environment

Staff members find disaster recovery planning to be a nebulous, frustrating, and ill-defined task; consequently, they do not readily attend to it. The key to circumventing this difficulty is to provide them with a conceptual framework that provides some structure to the seemingly insurmountable number of details. Conceptually, disaster recovery planning encompasses four distinct phases:

- Prevention and Preparation—implementing actions to avoid disaster or lessen its impact
- Prerecovery—making necessary arrangements and contacts in order to provide coverage following a disaster
- Immediate Recovery—taking actions to immediately restore computing capabilities
- Return-to-Normal Operations—restoring computing capabilities and work environment to their normal state

Historically, people have associated disaster with catastrophic events such as fires and tornados. The effects of several recent disasters, however, such as the Hinsdale Telephone switch fire, have caused people to think of disaster in broader terms. Rothberg [8] defines disaster as ". . .any event that causes significant disruption to operations, thereby threatening the business' survival." Therefore, our recovery planning efforts focused on providing a contingency plan for the failure of various types of services regardless of the cause. (See Table I.)

The following illustrates the issues that need to be

addressed in each of the four phases, some examples from our plan, and the role of the disaster recovery coordinator at each of these stages. (See Appendix 1).

Prevention and Preparation. During the prevention and preparation stage an assessment is made of the working environment and actions are implemented to avoid disaster or lessen its impact. Writers on the topic of disaster recovery planning state the first step is to determine which processes are critical [7]. Therefore, the major task of this phase is for each staff member to take a complete inventory of his or her job and determine critical applications. Once these critical applications have been identified, steps can be taken to prepare for or prevent a disaster.

A key element in the prevention phase is data protection. Almost all groups have some items that must be stored off-site and some that must be fireproofed in-house. Since this need does not vary, it would be inefficient and lack integration for each staff member to make individual provisions for the protection of his or her data. Therefore, the disaster recovery coordinator provides for this and other common needs. (See Table II.)

PCs have created special needs for disaster recovery. A quick survey of the staff at your facility will probably demonstrate that some staff members have backup copies of disks containing vital information, but these can probably be found in the same desk drawers as the originals. A disaster that destroys the original will very likely damage the copy as well. Temperatures of only 125°F as well as smoke can render a floppy unusable. Therefore, the purchase of fireproof safes designed especially for magnetic media storage should be included in the prevention stage.

The hard disks of many PCs also contain vital information. Ideally, hard disks would be backed up by the central computing center over the network during off-hours. Alternatively, the files can be uploaded to the mainframe and backed up by the normal mainframe backup procedures. For stand-alone PCs, hard disks can be backed up through the use of a portable tape backup unit.

The business office has special needs for data protection. While much of its information is contained on floppy disks, there is an abundance of important material (e.g., personnel records and performance reviews), that is kept only in paper copy. A separate fireproof safe is required to ensure the privacy of many of these records.

Provisions must be made for off-site storage as well as in-house storage. Preferably, this should be at a location that will not be affected by the disaster that disrupts the computer center, but should be close enough to make its use practical [3]. We have rented storage space at our campus foodstore's facility. This is a clean, environmentally controlled area suitable for the storage of magnetic tape. It is secure, yet accessible to our courier during normal working hours. We do a monthly full file backup and nightly incremental backups on all our machines. The most recent copy is kept on-site in a fireproof vault (designed to withstand 2000°F for 4 hours) and the previous version is taken off-site. A drop-box is located at the receptionist's desk in the main foyer so that employees may deposit items to be taken to the off-site location as they leave the building. Transport of items to the off-site storage location is provided by the regular computing center courier service.

Prevention and preparation are the crux of disaster recovery. The care and thoroughness with which this phase is implemented will determine how effectively recovery can be carried out in the event of an emergency.

TABLE I. Most Common Data Processing Disasters*

Water	22%
Power Failure	22%
Earthquakes	23%
Fire	9%
Communications	8%
Sabotage	3%
Other	13%

*Taken from Waas and Keen [9] Disaster's Top Ten.

TABLE II. Disaster Recovery Coordinator Tasks

Some needs in disaster recovery planning are so universal it would be inefficient and lack integration for each group to address these areas individually. These tasks should be addressed by the disaster recovery coordinator.

- Provide the conceptual framework for the organization and introduce the plan to the staff.
- Provide a facility for common off-site storage.
- Make arrangements for alternate compute power so that critical applications can be continued as soon as possible after an emergency.
- Provide for alternate workstations and office space so that the staff can relocate quickly and smoothly to begin the task of helping users recover.
- Compile the staff's sections of the document into the written disaster recovery manual and coordinate distribution.

Prerecovery. While preventative measures have been addressed in the previous phase, prerecovery encompasses those tasks, arrangements, or contacts which must be made in advance to ensure that effective recovery can begin in the event of a disaster. In this stage each staff member will assess what can be done to make recovery possible or easier. Diamond [3] points out that media restoration is always faster than replacement and can be done for 10 percent to 20 percent of replacement costs. Lists of vendors and other contacts and the services they provide can expedite matters in an emergency.

During the prerecovery stage decisions should be made about who will be in charge and what roles people will play in the event of a disaster [1, 4]. Concerns such as: who will notify the staff and where will they meet; who will be the spokesperson to deal with the

press and the users; and who will be called to make the damage assessment and determine if the alternate computer power location is to be contacted, should be addressed at this stage. This is the time for each staff member to take an inventory of his or her skills to determine whether he or she might be more useful in another area during an emergency [4]. For example, the person who usually works in instructional design might well serve a public relations function or help users become familiar with the off-site system. The goal of prerecovery is for each person to know what he or she is to do in the event of a disaster.

The prerecovery phase encompasses most of the disaster recovery coordinator's work: making provisions for where the computing will be done and where the staff can be relocated in case of an emergency. Realistically, subscription to one of the commercial hot-site, warm-site, or cold-site facilities is probably too expensive for an academic institution. Pastore [6] indicates that the hot-site cost for a medium-sized mainframe can be as much as $70,000 a year, a figure that is unacceptable to most universities. An apparent solution would be an agreement in which several institutions agree to provide backup for each other in case of an emergency. But most of the literature indicates these types of reciprocity arrangements do not work even though they are so widely promoted. The reason for this, according to Waas and Keen [9] and Pastore [6], is the partner will not have the resources "to spare" in the event of disaster. However, this statement is generally made in situations where each of the partners is a for-profit organization and ultimately will not be willing to give up prime-time cycles. Robbins [7] points out while reciprocity agreements are a problem with online systems, they were cost-effective and uncomplicated when batch systems were the norm. In an emergency, tapes could be loaded on the partner system and critical applications run via dial-up lines or networks during off-peak hours.

In larger institutions where other departments or sister campuses have their own computers, partnerships could be established with sites providing back-up for each other in times of emergency. Our institution established such partnership agreements with several academic institutions in the area.

A second important task facing the disaster recovery coordinator in the prerecovery phase is finding a site to which the staff can be relocated in the event of an emergency. An inventory of equipment minimally required by staff will assist in locating the site. An appropriate place to relocate from a central facility is an on-campus PC cluster. We have chosen to relocate to our combination Information Center and PC cluster. This location would provide a workstation for most of the full-time staff, printing facilities, and documentation.

Immediate recovery. Immediate recovery includes those actions which must be taken to restore immediate computing capability and work environment. The activities of this phase are very dependent upon the nature and extent of the emergency situation. The initial task, however, is to assess the extent of the disaster and decide how much of the plan will be implemented. It is crucial for this phase that notification procedures (which had been determined in the prerecovery phase) operate flawlessly and that staff know what is expected of them. Tasks that might be necessary in this phase include damage assessment, sending damaged media to be salvaged, notifying alternate compute sites of the disaster and preparing to run critical operations at the emergency location.

If the disaster requires computing to be done at the alternate site, it is likely that circumstances will not allow everyone to use this facility. A determination of critical users must be made. This could be a very sensitive issue and perhaps should not be addressed in the emotional turmoil of a disaster. In our plan, the Dean for Academic Computing determines who the critical users will be. This decision is based on such factors as the availability of resources and the time of the academic year during which the disaster takes place. Other options include giving priority to specific content areas (such as medical research); applications area status (senior-level courses, dissertation work, funded grants); or user status (faculty, staff, student).

People who have experienced a disaster say they are surprised at the impact the emergency has on the staff. The stress factor generally appears 90 to 120 days following the disaster [1]. It is imperative that staff members have a means of support and a way to ventilate. It is also important for people not to work excessive hours. In emergencies everyone wants to do as much as they can, but for things to run smoothly over the long-term it is important that people maintain a normal working schedule.

Return-to-Normal Operations. Return-to-normal operations includes all those steps necessary to restore computing capabilities and work environment to their pre-disaster state. This includes activities such as the purchase of new computers, restoration of facilities, and return of users to original computing environment. This is often the most difficult phase to plan because so many aspects of it, including funding, are contingent upon the type of disaster encountered and decisions beyond the computer organization itself. Additionally, a disaster might be an opportunity to scrap plans for incremental changes to aging systems in favor of major strategic changes. Therefore, creating a realistic disaster recovery plan may require that this phase be addressed only superficially. The plan we developed did not encompass this phase in the initial planning, but may address these issues in future revisions.

Implementing the Plan into the Organization

The disaster recovery coordinator's primary function is integrating the plan into the organization. Once the conceptual outline has been developed and senior management has announced disaster recovery as a priority, the planning process is ready to be introduced to the

staff. It is useful for the disaster recovery coordinator to meet with each group to present the conceptual outline, review the common needs provided by the coordinator, and outline the steps involved in compiling the disaster recovery manual (See Appendix 2).

In our process, each individual wrote a personal disaster recovery plan and submitted it to his or her manager. This provided some incentive for each staff member to take the task seriously and ensured that each plan would be reviewed by someone who was familiar with the individual's job. Managers then integrated these sections into a chapter for inclusion in the written disaster recovery manual.

We devised our plan around the existing organizational structure. In stressful situations people work best in a familiar environment. Each group should remain intact and report to the customary people. This structure also places the onus for the disaster recovery plan on the managers who control staff time rather than on the disaster recovery planning coordinator who has no such authority.

LESSONS LEARNED

Rothberg [8], Morris [5], and Janulaitis [4] all note that senior management support is a critical element in the success of the plan. Our experience confirms this. A comprehensive plan requires each individual within the organization to invest the resources to take a complete inventory of his or her job and carefully consider how the plan will apply to his or her situation. This is time away from normal day-to-day activities, special projects, and deadlines. For staff to take the assignment seriously, it must be clear that management has made a commitment to the development of a plan and expects active participation.

Senior management support is also necessary because disaster recovery is a *cost* to the organization—in terms of time, money, and human resources. We developed and implemented our plan in six months with the disaster recovery coordinator working half-time on the project. We spent nearly $13,000. (See Table III.)

But the costs do not stop here. We estimate that keeping a plan up-to-date will take an ongoing 10 percent of the disaster recovery coordinator's time with an additional two weeks per year for an intensive review and update. He or she will need to solicit revisions or additions from staff members, update the plan and distribute revisions for inclusion in the written disaster recovery manual, and coordinate and supervise periodic testing.

Maintaining the plan will make demands on other staff members' time as well. The computer center courier service will be permanently affected by the additional transportation to the off-site location. Staff will need to take time to make backup files and make regular revisions and additions to their individual portions of the plan. Ongoing disaster recovery planning will require time and resources since it should be integrated into many areas, including operating budgets, capital budgets, and project management. Ideally, integration of disaster recovery planning as an on-going part of projects will decrease recurring effort required as well as improve the quality of the disaster recovery plan.

TABLE III. Approximate Costs

Units	Item	Unit Cost	Total Cost	Yearly Cost
1	Weather Receiver and Adapter	$ 50	$ 50	$ ___
1	Tecmar Qic60H Tape Backup Unit	1,297	1,297	___
50	PC Boards for Tecmar	88	4,400	___
20	Tecmar Tapes	25	500	500
2	Fireproof Media Vaults for On-Site	699	1,398	___
1	Fire Proof Paper Cabinet for On-Site	850	850	___
	Magnetic Tapes for File Back-up	2,850	2,850	___
4	Transport Cases for Tapes	199	796	___
6	Transport Cases for Floppies	40	240	___
	Rental Fee for Off-Site Storage Space			736
			$12,381	$1,236

Despite continuing costs, in some ways the development of a disaster recovery plan may be easier at an academic institution than a commercial one. An academic institution can capitalize on existing resources. The existence of a college union often insures the close proximity of needed support services. Public terminal and PC clusters provide readily usable resources that are already maintained for daily use and consequently do not require an additional burden that would be used only in case of disaster. While these resources do not make the plan easier to create, they provide the advantage of quick and easy access that can serve a dual purpose at little additional cost.

Academic computing centers also have the advantage of not generally being required to bring in funds for the continued short-term running of the college or university. Consequently, in case of disaster, an academic computing center may well be in the desirable position of having the time to briefly delay its recovery in order to thoroughly review its plans with an eye toward significantly leapfrogging its technology and strategies.

The computing center staff members do not find disaster recovery planning an easy or interesting exercise. Many have little time or interest to invest in something so obscure. Therefore, it is essential the disaster recovery coordinator not be held responsible for the disaster recovery work of the staff. The disaster recovery coordinator can guide and integrate, but the thoroughness and accuracy of the plan rests with each individual.

Encouragingly, while disaster recovery planning has been a neglected topic in the past, Colby [2] points out that since recent graduates in computer science have learned of the importance of disaster recovery, we may find a new attitude emerging.

We believe there are several points that should be added to our disaster recovery planning. First, while we have done isolated tests, we have not done a full-scale mock disaster and we believe we should. Testing is the phase in disaster recovery which is commonly overlooked. Colby [1] notes in a Texas study of companies having experienced disasters, the plan had never been tested in 95 percent of the firms that had established plans. Second, we would like to add disaster recovery planning to all new projects. We believe disaster recovery planning should be a standard part of the project planning process just as software licensing and documentation are. Finally, we would like to develop a file backup service for our users. Ideally this would be done through a network, but this is not a viable alternative for floppy disks or stand-alone PCs. We would like to offer a mail-in or drop-in file backup service. A user would mail a tape, floppy disk, or cartridge tape to the computing center in a self-addressed campus mail envelope. The article would be stored until needed. We are, however, concerned about campus mail providing the proper security and physical environment.

While varying circumstances at each academic institution will require disaster recovery planning unique to that environment, the structural framework and stages of recovery outlined here should provide the direction necessary for planning at any institution. Planners will find the preceding information makes it possible for them to present an organized and well thought-out system for implementation at their sites. Success, of course, depends on the thorough and committed utili-

APPENDIX I.
Typical Tasks at Each Stage in Disaster Recovery

I. Prevention and Preparation
- Determine critical applications
- Protection from water, fire, etc.
- Data protection
- Off-site storage

II. Pre-Recovery
- Provide for alternate compute power
- Provide for alternate work environment
- Identify and record needed resources (e.g., media salvaging)
- Determine emergency sequences (where to meet, who to call, etc.)
- Determine who will play what role in an emergency
- Identify skills of staff not normally "used"

III. Immediate Recovery
- Contact alternate compute facility, prepare to run applications
- Move staff to alternate location
- Determine critical users
- Provide training for users on computing at alternate site
- Damage assessment
- Media salvage
- Regulate work schedules
- Provide emotional support

IV. Return-to-Normal Operations
- Restoration of facilities
- Purchase of new computers or clearance to use old ones
- Return users from alternate compute site to home machines
- Increase insurance coverage?

APPENDIX II.
Welcome to Disaster Recovery

Our mission as coordinators of the evolving Disaster Recovery Plan is to help you identify and organize the critical aspects of your working operations and to help you think ahead to do everything we can in order to recover quickly in the event of a disaster. We think the following outline will help.

Imagine for a minute that when you come to work one morning, the building is not usable. The sprinkler system was inadvertently activated and could not be shut off. You are assigned workspace that consists of an empty room. What do you need to get critical applications running? What do you need to get back to "business-as-usual" and in what order?

I. Identification of Critical Operations vs. Long-Term Recovery
- What functions and applications need to be resumed immediately?
- What files and materials do you need immediately?

II. Back-up of Critical Information
- What are the critical things that you have assumed will always be there in the morning?
- Have important, time critical mainframe files been dumped to tape?
- Are important files on floppy disks backed up and stored in the fireproof media safe?
- Have you backed up vital data, programs, contracts, and licenses?

III. Off-Site Storage and Back-up of Materials
- Have tapes and floppies been stored at the off-site location?
- Are the materials clearly identified, dated, and periodically updated?
- Have you backed up your customized working environment (e.g., Kermit initialization files)?
- Are materials specific to an individual or group backed up?
- Does each person have a copy of the plan at home and do they know what their responsibilities are if the plan is activated?

IV. Hardware Inventory
- Identify the hardware needed to address critical applications.
- Can some functions be performed at home on your own personal equipment?

V. Bibliography
- List documents, books, manuals, and other references needed for critical applications.

zation of this information; but the framework suggested here is the instrument for mastering the initial difficulties.

REFERENCES

1. Colby, W. Burnt or burned? *Inf. Syst. 32*, 2 (Feb. 1985), 40.
2. Colby, W. Disaster recovery plan? Nah,. . .it'll never happen to us! *Inf. Syst. 32*, 10 (Oct. 1985), 32-36.
3. Diamond, S. Computer disruption:Planning for the worst. *HighTech. 7*, 5 (May 1987), 54–55.
4. Janulaitis, M. V. Creating a disaster recovery plan. *Inf. Syst. 32*, 2 (Feb. 1985), 42-43.
5. Morris, D. Do's and don'ts of customizing recovery. *DG Rev. 9*, 6 (Dec. 1988), 46.
6. Pastore, J. That phone call. *DG Rev. 9*, 6 (Dec. 1988), 35-38.
7. Robbins, R. M. Taking the disaster out of recovery. *Inf. Syst. 33*, 7 (July 1986), 38-44.
8. Rothberg, M. L. Disaster plans:Added Complexity. *Comput. Dec. 21*, 2 (Feb. 1989), 16.
9. Waas, W. and Keen, J.S. Disaster's top ten. *DG Rev. 9*, 6 (Dec. 1988), 43-50.

CR Categories and Subject Descriptors: E.5 [**Data**]: Files—*backup, recovery*; K.6.4 [**Management of Computing and Information Systems**]: System Management—*management audit, quality assurance*; K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*security*

General Terms: Management, Security

Additional Key Words and Phrases: Backup files, recovery, system management

ABOUT THE AUTHORS:

RENATE ROHDE is assistant professor of education at Oakland University in Rochester, Michigan. Her special interests include statistical computing and the applications of computing in education. The work for this article was done while she was employed as senior applications and capacity planning programmer at Bloomington Academic Computing Services at Indiana University. Author's Present Address: Counseling Department, Oakland University, Rochester, MI 48309.

JIM HASKETT is director of computer services at Central Washington University. His current interests involve computing center management in academic institutions and computing for the future. The work for this article was done while he was manager of the Performance Analysis and Capacity Planning group at Bloomington Academic Computing Services at Indiana University. Author's Present Address: Computer Services, Central Washington University, Ellensburg, WA 98926.