

## **IT Disaster Recovery Planning**

**Bill Ramsay**  
**Information Systems & Services**  
**Berea College**  
**CPO 2208**  
**Berea, KY 40404**  
**859-985-3342**  
[bill\\_ramsay@berea.edu](mailto:bill_ramsay@berea.edu)

### **Introduction**

As higher education business and learning processes have become more and more dependent on computer technology, protection of those resources from risk has become a major challenge for college and university IT departments. The challenge has become more complex as the technology has become decentralized, involving nearly every person in an institution in computer operations to some degree and creating many possible points of failure. IT professionals logically become wary, always looking over the shoulder for the inevitable. What risks could break down the technical infrastructure and how would that affect the operation of offices and classrooms? How prepared are we for the possibility that a physical disaster, equipment failure, vandalism or operator error could compromise data integrity, data confidentiality or processing availability? How high is the risk? Could we recover? A formal disaster recovery plan can provide a foundation for continually improving management of risks, preparedness and recovery resources.

Disaster planning can be broken down into four focus areas - risk management, business continuation strategies, preparedness activities and recovery planning. A well-rounded plan will address all four areas and will be periodically reviewed to maintain accuracy and to identify opportunities for improvement. This paper will discuss each area and then present a plan document outline that the reader may find useful in beginning his or her own planning project. It should be noted at the outset that our subject is disaster recovery planning such as an IT department would logically undertake. We will endeavor to help the reader understand the elements of a sound risk management and recovery planning effort. We are not attempting to address the broader issue of business continuity planning in which the entire institution would review threats and contingencies for information and communication technology along with risks to other infrastructure, financial or personnel resources.

### **Terminology**

To reduce the risk of confusion, we'll start by defining some terms that may be unfamiliar to some or that may be used in this paper in a particular way.

Disaster recovery planning. Establishment of plans and strategies that would facilitate recovery from damage to information and communication technology infrastructure within a time frame that the business could tolerate.

Business continuation strategies. Establishment of plans and strategies that would allow critical business functions to continue during a recovery period in which informa-

## *2008 ASCUE Proceedings*

tion and communication technology infrastructure is impaired due to a disaster event.

**Disaster event.** Any occurrence which results in significant disruption to business and/or learning processes which are dependent upon information and communication technology infrastructure.

**Information and communication technology infrastructure.** The computer and networking equipment, software and procedures that support the business activity of an organization.

**Recovery Resources.** Documents, software installation media, data backup media and other items kept on hand, preferably in protected storage, which would be needed by technicians charged with rebuilding damaged systems on replacement or interim hardware.

**Hot Site.** A set of facilities and equipment kept on standby and ready for use as an interim processing location by an organization recovering from a disaster event.

**Cold Site.** A space provided with network cabling and power into which replacement or interim equipment could be installed for use as an interim processing location by an organization recovering from a disaster event.

**Recovery Time Objective (RTO).** The goal for elapsed time from declaration of a disaster event to restoration of essential operations that has been agreed upon by an organization as an acceptable parameter for disaster recovery planning.

### **Risk Management**

So what are the risks? What can we do to prevent them? What can we afford to do? What should the priorities be? A review of possible risks and consequences is a good place to start our planning. While we are doing so, we will do well to identify which are more likely to occur and which will do the most damage to our operations. Then when we think about risk reduction strategies, we can set higher priority on risks and consequences that would do a lot of damage and are more likely to occur. There are always other areas to consider, but we'll discuss ten risks and four areas of possible loss. Risks include infrastructure failure, hardware failure, accident or vandalism, cyber attack, fire, water damage, software failure, loss of access, operator error, and knowledge loss. Consequences may include loss of data, loss of processing, loss of availability, or loss of confidentiality. Of course, every disaster is unique and a major disaster event such as Hurricane Katrina could cause problems in many areas. However, if we have examined each area separately, we will be more able to deal with them if they happen all at once. In addition, we need to remember that most of the disasters we will be called upon to deal with will be small, but many of our prevention and recovery strategies apply to all types of events.

**Risk – Infrastructure Failure.** A 2007 study reported that the most common cause of disruptive events among higher education institutions surveyed was infrastructure failure. Of the institutions reporting a disruptive event, 82% had experienced an electrical failure and 60% had experienced a failure of cooling or other environment control systems. In addition, 81% of electrical

failures and 57% of environment control failures impacted many business process or the entire campus.<sup>1</sup> The impact of environment control failure is well known to us at Berea College as we found a few years ago that when the server room cooling system failed, equipment began overheating within an hour or two, even in winter. During an extended electrical outage our backup power system was able to keep servers running for several hours, but they had to be shut them down because there was no backup power for the cooling system. Another area that may be overlooked is electrical circuit capacity. As equipment changes are made, loss of power due to circuit overload has been a frequent problem in my experience. Risk reduction strategies would include battery or generator based backup power systems, supplemental cooling systems for server rooms and network hub spaces, redundant cooling equipment, temperature threshold warning devices and buffer capacity in electrical circuits.

Risk – Hardware Failure. The study referenced above found that hardware failure was the second most common cause of disruptive events, reported by 72% of institutions. Breadth of impact was less than that of infrastructure failure, with 48% of incidents affecting many business processes or the entire campus.<sup>2</sup> Hard drives and power supplies are the most common server components to fail in my experience, but other components such as network interface cards and memory have also caused problems. Risk mitigation strategies include RAID disk configurations, redundant power supplies, redundant network interfaces, spare parts inventory and parallel servers with failover capability.

Risk – Accident or Vandalism. The most common accident reported in the 2007 ECAR study was cable cut – reported by 51% of institutions reporting a disruption and not surprising given that most college campuses consist of multiple buildings connected by lots of buried copper and/or fiber optic cable. Theft, which could be considered a form of vandalism, was experienced by 19% of institutions reporting a disruption in that study.<sup>3</sup> Prevention strategies include maintaining cable location maps, setting up redundant cable paths, requiring IT staff to be present at digs and establishing good access control mechanisms for spaces containing critical equipment.

Risk – Cyber Attack. The incidence of disruption by cyber attack reported in the 2007 ECAR study was equal to that of cable cuts, but the impact was lower with 48% of events affecting many business processes or the entire campus.<sup>4</sup> Cyber attacks would include virus outbreaks and denial of service attacks. Prevention measures to consider would include Internet firewall, anti-virus software, network access control systems, intrusion detection systems and automation of workstation software updates.

Risk – Fire. While fire is not as high a risk as some other areas, the potential for widespread harm to infrastructure, equipment and personnel make it worthy of investment in prevention. Strategies include HALON or other automated extinguishing systems for critical spaces, alarm systems, and training of personnel in standard fire prevention practices relating to electrical cords, trash disposal, smoking, etc.

Risk – Water Damage. Roofs leak, pipes burst. I've never experienced a fire, but I have run into water problems here and there. In one incident in a past job, leaking air conditioner plumbing allowed water to build up under a raised floor and we didn't know about it until suddenly our phones stopped working. A water sensor under the raised floor would have alerted us to the problem before any disruption occurred.

## *2008 ASCUE Proceedings*

Risk – Software Failure. Software bugs can corrupt data, present false information or break down processes. Software companies can go out of business or change policies and leave users with no recourse when problems occur or revisions are required to remain compatible with an operating environment. Disciplined software acquisition and change management processes, software maintenance upgrade contracts and source code escrow are strategies that can mitigate the risks.

Risk – Loss of Access. I recently attempted to pick up a family friend to attend an event and found several blocks around her apartment cordoned off by the police due to a gasoline spill at a service station. I heard a story from Hurricane Andrew in which company IT personnel rented a helicopter and landed on the roof of their building in a flooded area to retrieve backup tapes so recovery processes could be started at an alternate site. While we probably won't maintain a standby helicopter, we do need to think about where problems would occur if we could not gain access to some or all of our facilities. Options for reducing the potential consequences of access loss would include VPN services, avoidance of processes requiring an operator's physical presence, offsite storage of backup media and other recovery resources, and hot site contracts or reciprocal agreements.

Risk – Operator Error. People make mistakes - to err is human. Procedural errors, accidental file deletions, failure to perform data backups, and other operator errors constitute a risk within our information and communication technology infrastructure. With the expansion of personal computers as an integral part of institutional data stores and processes, the possibilities for operator error have increased. Automation of processes, process design that includes verification steps, documented procedures and central storage of "official" data files may help reduce the risks.

Risk – Knowledge Loss. One of the most challenging risks to manage is personnel turnover. Information and Communication Technology systems often require intervention by individuals with specialized knowledge, and if one or more of those individuals are suddenly unavailable due to a disaster event, a personal situation or departure from the staff, the systems may become inoperable. Documentation of system startup and shutdown procedures, configuration options and administrator passwords, cross training of staff and development of vendor partnerships may be considered as ways to manage this risk.

Consequence – Data Loss. A professor's hard drive crashes. He or she has not made a data backup for over a year, so valuable research data or curriculum development is lost and the time and money invested produces no return. How can we protect ourselves in the new world in which everyone is a computer operator and important data is stored in hundreds of locations? Provision of central data storage with sound backup and archiving processes can help. Relentless exhortation and training of PC users in data backup techniques can help, as can provision of PC backup processes that are easy to use. Some may want to consider enterprise backup software or Internet service that automates server and PC backups. Some data may be volatile enough and critical enough to merit maintaining a frequently or continuously updated parallel copy on another server or off site.

Consequence – Processing Loss. When technology infrastructure services are disrupted, processes are halted and delays in decision making or transaction processes can occur. Encouraging users to request information earlier than the last minute can reduce the impact of an interruption.

Developing standby procedures that allow transactions to be accepted for later completion is another useful strategy.

Consequence – Availability Loss. The data may be all there and the computers all running, but if the network is down or people can't enter their office building for some reason, decisions and transactions will be impacted. Designing systems with alternate methods of access and the same procedure design and operations schedule ideas noted in the previous paragraph may reduce the consequences.

Consequence – Confidentiality Loss. Recent incidents in the news of large quantities of social security numbers being exposed due to laptop theft have highlighted the possibility that a disaster event can have low impact on data, processing or availability but high impact on business due to loss of data confidentiality. Encryption of confidential data, good access security practices and training of PC users can be considered as strategies to minimize these losses.

### **Business continuation strategies**

Once a disruptive event has occurred, even with the best of plans business as usual will not be possible for a period of time. It is important that we think about how business will be conducted during the recovery time, and how long that period can reasonably last. IT departments cannot develop detailed contingency procedures for other functions, but our planning effort can identify at least some portion of critical transactions and suggest approaches our colleagues might utilize. We also want to recognize that some systems are more urgent than others and those systems should be restored first. An inventory of functional systems combined with a thought process that identifies those that are critical can help guide the focus and sequence of our recovery efforts.

Recovery Time Objective. A disaster recovery planning strategy is based on an initial decision regarding how long the business could reasonably operate with significant breakdown to information and communication technology infrastructure. Could we operate for two weeks, or do we need capability to recover in two days? Are there some systems that need rapid recovery while others could wait for several weeks? Once a Recovery Time Objective is agreed upon and essential functional systems identified, backup procedures and recovery plans can be developed that would support the objective.

Functional Systems Inventory. Most classic disaster recovery planning literature recommends a detailed inventory of all functional information and communication systems. Starting with this inventory, we then identify the detailed technical infrastructure upon which each functional system depends. Then we rank the systems by importance and let that drive the risk management and recovery planning for the technical infrastructure components. The difficulty is that we will never get it done if it is that complicated. A simple list of major functional systems is achievable and adequate. Classifying systems as Essential, Important, or Convenient will give us a useful and attainable division to guide our recovery efforts. Accounts Payable might be considered essential because we have to pay our bills. A course management system might be considered important, but it is not essential because professors can continue to conduct classes for a week or two without it. A digital library resource server might be considered convenient because research plans can be rescheduled.

## *2008 ASCUE Proceedings*

Interim Transaction Processing Plans. Within each major functional system, key high volume transactions can be identified for which interim processing procedures would be necessary during a disaster recovery period. IT analysts along with client department partners can readily identify and list those transactions and suggest a logical approach for interim processing from among the following options. The thought process involved in developing a best effort list will make staff more able to address all needed transactions in a disaster scenario.

Source Document Staging. Accept source documents such as admissions applications or transcript requests and stage them for later processing once the systems are available.

Paper Filing. Set up a temporary filing system so documents can be executed and/or accepted and filed for later retrieval as part of other procedures and ultimately for data entry once systems are available.

Manual Process. Electronic forms can be temporarily replaced with paper forms which can be routed for approval or other action and possibly staged for later data entry.

PC Process. A spreadsheet log may be used to collect transactions or record activity and later used to drive catch-up data entry.

Alternate Process. Sometimes an alternate process is already in existence that may be operational. For example, direct deposit may not be functional, but we could print payroll checks instead. Or our Accounts Payable system may be down, but we could hand write checks.

Alternate Location. Some transactions may become operational if moved to an alternate location. For instance, if the campus phone system is down, calls could possibly be made from home or from a mobile phone.

### **Preparedness Activities**

What can we do to be ready for whatever happens? What would we need to know and to have on hand if we had to rebuild damaged databases or infrastructure? Preparedness activities involve maintaining an appropriate set of recovery resources and training users and IT staff in readiness and recovery procedures.

Recovery Resources – Data Backups. Data backup processes are the cornerstone of any recovery plan. Each functional system or database will have its own logical parameters for backup processing based on data volatility and value. The more volatile data is, the more frequently a backup copy must be made to support acceptable recovery quality. The more necessary data is to organizational functions, the more important it is to verify the validity of backup processes and to protect backup media from loss. Data which does not change, such as a photo archive set, can be copied to DVD or other media once and stored off site. Critical data which changes constantly may need to be maintained in full parallel at an offsite location. Most data will be somewhere in between. Each data backup medium has advantages, disadvantages and special considerations. Tape media ages and must be replaced every few years even if the data has not changed. CD or DVD media may not be readable on all recovery systems. Disk arrays may not be allowed into a commercial hot site or recovery center. Internet backup services may not be

verifiable. A good disaster recovery plan will document the backup media types, refreshment frequency and locations for all functional systems.

Recovery Resources – Software Installation. When servers or PC's are lost in a disaster event, software will need to be installed on replacement equipment. Our recovery resource set needs to include original installation media or backups that would allow software configurations to be rebuilt. Use of server virtualization and hard drive imaging techniques can be a useful and time saving technique for providing software installation recovery resources. A complete list of these resources needs to be a part of the disaster recovery plan document.

Recovery Resources – Information. Rebuilding servers, software, routers, switches, etc. will require many configuration options to be set. We will not be able to rely on our memory for these options. Documentation, whether paper or electronic, of configuration options, passwords, Internet URL's, IP address schemes and other details must be a part of our recovery resource set. In a past technical job, I restored the operating system of an IBM AS/400 only to find that the tape was old enough to include an earlier system administration password which was no longer on record. Since that time, I keep a list of former passwords on file. Another set of information that will be needed is vendor contacts. In the time crunch of responding to a disaster event, a quick reference of vendor partner contact information would be very useful as part of the plan document or as a recovery resource.

Recovery Resources – Auditing. Disaster planning is of no value if we do not do what we plan. Periodic audits can verify that all listed recovery resources are found in their proper places. Results of these checks would be a logical exhibit to show in an annual financial audit which includes a review of IT practices. Testing of risk reduction systems such as uninterruptible power and alarm systems should also be a part of standard operating procedure. The disaster recovery plan documents should include a list of routine testing and audits planned and record the individuals responsible for following up.

Training and Communication. Disaster readiness is everyone's business, so a successful planning initiative will involve reminding everyone of the fact. I recommend that at least once per year, a reminder be sent to all personal computer users reminding them of their part in being sure data is stored in proper locations and is being backed up according to policy. All faculty and staff also need to know how to report a suspected disaster incident and how a response decision will be made. An annual reminder for folks who have specific responsibilities to maintain readiness or as part of a response can encourage them to read the plan and verify that audits, backups or other activities are happening. An occasional workshop or disaster mock-up event might also be helpful. The schedule for routine reminders along with training materials would logically be included in the disaster plan document or recovery resource set.

## **Recovery Planning**

Planning ahead can save significant time and reduce the risk of false starts in a disaster scenario where time is likely to be very precious. Recovery events follow a common life cycle and thinking about the stages of that cycle in advance will help us if we are ever involved in an IT disaster recovery. We can also benefit from defining in advance who would be responsible for various aspects of a recovery sequence and by notifying those individuals and offering training to them.

Finally, we can test our plans, knowledge and recovery resources for adequacy and completeness.

Recovery Life Cycle. The recovery cycle documented in a formal disaster recovery plan cannot be a comprehensive task list or instruction set. It can be a useful guide to the detail planning that must occur to effectively coordinate a recovery effort. It will help participants to remember key areas that may otherwise be overlooked in the crunch of a recovery scenario. Each disaster event is unique in its specific impact and recovery requirements, but a common set of considerations can guide the unique detail planning that would be required. Following is one way to look at the sequence of events that must occur in a recovery.

Incident Reported. Our planning needs to define and our communication needs to instruct faculty and staff how a suspected disaster incident should be reported. A practice I have seen used to good effect is to ask site security personnel to be the recipient of reports, and provide them with instructions on how to notify IT decision makers for follow-up.

Disaster Declared. A decision process is needed which evaluates and confirms a reported incident and determines if disaster recovery procedures need to be invoked. Once the decision is made, the recovery team will be notified and a detailed assessment can begin. A central location for recovery team work and meetings will likely be established. This stage will also include communication to faculty, staff, students, executive administration and public relations.

Safety Evaluated. Many disaster scenarios will involve damage to or contamination of a physical space. Before any IT personnel enter such a space to begin damage assessment or to perform recovery activities, safety professionals will need to evaluate the situation and determine whether access restriction is required and whether medical or rescue services need to be invoked.

Damage Assessed. As soon as is possible, a full report of infrastructure damage would be assembled by the Recovery Team and provided to the CIO/IT Director and the institution's executive administration.

Interim Transaction Procedures Invoked. Once damage assessment is complete, operational departments can be notified of the specific areas that have been disrupted. They can then set up and coordinate interim transaction processes.

Task Groups Established. Recovery Team members will assemble task teams to begin recovery of various systems or infrastructure segments, depending on what has been disrupted. Administrative and logistical support for the recovery teams will also need to be set up so they will be able to focus on recovery actions while others take care of placing orders for equipment, obtaining supplies, providing food, etc.

Detail Plans Completed. The Recovery Team and task groups will develop a detailed plan for acquisition of equipment and services, replacement equipment installation and recovery action steps. The plan must be reviewed and approved for necessary funding by the CIO/IT Director or the institution's executive administration.

tion, depending on the level of funding required. Communication to faculty, staff and students of the recovery plans and of progress as the recovery continues will be an important part of the plan.

Equipment and Services Procured. Unless a hot site contract is in place which provides access to standby equipment, procurement of replacement equipment will be a critical path activity in the recovery plan. Rapid identification of equipment to be purchased, availability of vendor contact information among the recovery resource information documents, and assignment of administrative support personnel to aggressively follow up on the acquisition process will be important to minimizing the time required. Services may also be required due to technical expertise not being available among local staff or in order to augment staff capacity and accelerate the recovery. Coordinating approval of statements of work and service contracts will be a part of the acquisition activities. Through all this process, it is important that careful records of expenses and copies of source documents are kept to support possible claims against insurance policies.

Restoration Site Determined. As resources are assembled, a decision will need to be made regarding the location for setting up restored essential services. In many scenarios, a repaired or partially repaired original site will be used. If a hot site or cold site contract is in place, the use of those facilities may be preferable. If the original site is unusable, some alternative site plan will be required. If an alternate site is set up, provision must be made to move salvageable equipment to the alternate site as well as to deliver replacement equipment there. A related possibility is that temporary work spaces for personnel may need to be established so they can operate business functions once essential services are available.

Essential Services Restored. Recovery efforts will focus on restoration of those services identified in the plan as essential. Once production operation is restored, data backup procedures will need to be resumed. Backup media utilized for recovery need to be returned to offsite protected storage as soon as possible. Service users can then be informed of system availability and they can resume normal processing procedures and begin any required catch-up transaction processing.

Normal Operations Restored. If alternate processing or work sites have been set up. Activities will be required for completion of repairs to original sites and relocation of equipment and processing to the repaired sites. As non-essential services are restored, further communication and business procedure restarting will be needed. Long range plans may have to be set up for rebuilding some services that are lower priority or that cannot be put in place for some reason before normal operations have resumed. An official decision and announcement will be in order, declaring the end of disaster recovery operations.

Follow-up Activities Completed. Insurance claims and regulatory reporting may need follow-up after normal processing is restored. A review of the disaster recovery plans to make revisions that account for what was learned from the incident will be useful.

Recovery Organization. Preplanning the assignment of responsibilities for aspects of a disaster event response is an investment that can save time during a recovery. Typically the recovery team will be chaired by senior IS leadership and composed of members of IS organization assisted by a few others. Berea College's recovery team includes the CIO, Network Services Coordinator, Director of Administrative Systems, Computer Center Director, Instructional Technology Coordinator, VP of Finance, SGA President, and an Administrative Assistant.<sup>5</sup> Berea's plan also documents the names and phone numbers of individuals currently in each position.<sup>6</sup> Recovery team members would assemble task groups for each of their areas gathering the expertise required by the particular scenario being addressed. The disaster recovery plan will also document the areas of responsibility for each recovery team member. Responsibilities that need to be addressed include actual recovery of various technology areas, communication with the campus community and the public, and logistics of order placement and recovery task group support.

Recovery Testing. Short of experiencing a disaster, the best way to find ways to improve a disaster recovery plan is to test all or a part of it. The simplest way to provide for testing is through a hot site contract which includes blocks of test time using the standby equipment. Most small schools will not be able to afford a hot site contract, though. A minimal approach would include occasional verification that data could be restored from backup media. At Berea, we maintain a log of incidents in which a specific file restore is requested due to accidental deletion or for historical research. The log is presented as evidence of minimal testing of the recovery plan. We'd like to do more, but have not yet found a way we're willing to commit to.

Continuous Improvement. An annual review of the disaster recovery plan can be a sound basis for continuous improvement. Risk reduction strategies that have been considered but not implemented can be documented in the plan and reviewed each year for possible implementation. Testing strategies can be reconsidered. Preparedness actions can be audited and documentation of equipment, contacts and backup procedures can be brought up to date.

### **Sample Disaster Recovery Plan Outline**

- I. Executive Summary – Outline the reasons, goals, recovery time objective, and basic approach to the planning.
- II. Overview – Discuss more completely the rationale and philosophy behind the plan, report infrastructure components not covered by the plan, list the major systems and services addressed by the plan, and list the kinds of disaster events considered in the plan's development.
- III. Prevention Strategies – Document the policies, infrastructure options and procedures that have been put in place to reduce the risk of disruption due to a disaster event. List the strategies that have been considered but have not been implemented. Including the estimated cost of implementation can help a reader understand the decision.
- IV. Readiness Procedures – List the ongoing backup, testing, audit, communication and training activities that are expected to happen in support of the plan.

- V. Recovery Team – Document the organizational structure and membership of the recovery team, the responsibilities for each position and the name and contact information for each person.
- VI. Recovery Process – List the steps of a recovery life cycle and outline the activities or deliverables for each one. List the major functional systems that may need to be addressed and identify which are considered essential for restoration within the recovery time objective. Document the types and storage locations of backup media and the vendor contacts to be utilized for obtaining replacement equipment. Describe the content and location of recovery resources for each major system addressed by the plan.
- VII. Business Continuity – Describe the approaches that could be taken for contingency business procedures. List the critical transactions identified as part of the plan and recommend approaches for interim processing during the recovery period.
- VIII. Appendices – Variable information such as vendor contacts and information requiring frequent reference during recovery such as the list of recovery resources can be pulled out of the plan body and referenced as an appendix. The appendices then become a quick reference for information required in a recovery scenario, and are the focus for the annual updates that keep the plan current.

## **Conclusion**

Murphy's law states that if something can go wrong, it will go wrong. IT staff are very familiar with that law. A formal Disaster Recovery Plan can build resources that counteract it to some degree. Risks can be avoided and consequences mitigated by considering and implementing risk management strategies. Business impact can be reduced by planning for contingency procedures. Recovery from events that do happen can go smoothly because we have planned ahead and have maintained preparedness. With a modest investment in planning, we can live with less stress and sleep better at night.

## **Resources that may be of interest:**

List of disaster prevention technologies

<http://www.epriweb.com/public/000000000001000427.pdf>

EDUCAUSE ECAR study of disaster recovery planning practices in Higher Education

<http://connect.educause.edu/Library/ECAR/ShelterfromtheStormITandB/39105>

Berea College Disaster Recovery Plan document

<http://www.berea.edu/iss/documents/ISSDisasterRecoveryPlan.pdf>

Abilene Christian University Disaster Recovery Plan document

<http://www.acu.edu/technology/is/recovery.html>

## *2008 ASCUE Proceedings*

Oakland University submission to EDUCAUSE Effective Practice library  
[http://www.educause.edu/Browse/705?ITEM\\_ID=218](http://www.educause.edu/Browse/705?ITEM_ID=218)

DRI web site  
<http://www.drii.org/DRII/>

Disaster Recovery Journal web site resources page  
[http://www.drj.com/index.php?option=com\\_content&task=view&id=751&Itemid=428](http://www.drj.com/index.php?option=com_content&task=view&id=751&Itemid=428)

Virginia Tech's list of IT disaster possible consequences and prevention strategies  
<http://www.security.vt.edu/ITrisks.html>

Chronicle of Higher Education 2003 article on disaster recovery planning  
<http://chronicle.com/free/v49/i25/25a03301.htm>

### **References:**

1. Ronald Yanosky, ECAR, "Shelter from the Storm: IT and Business Continuity in Higher Education," 2007, pages 112-113
2. Ibid.
3. Ibid.
4. Ibid.
5. "Disaster Recovery, Business Continuity, and Network Redundancy Plan," Berea College, 30 May 2007, page 10 <<http://www.berea.edu/iss/documents/ISSDisasterRecoveryPlan.pdf>>
6. Ibid., page 16