

Disaster Recovery Planning – The Process

Introduction

We began our planning processes after experiencing several disasters, including a building fire, an environmental contamination, faulty discharge of a fire suppression system, and several severe electrical outages. This document describes the process that we use to evaluate risk and plan for recovery from disaster. It is an ongoing process, not a destination. It is impossible to document everything needed for every disaster recovery. Plan on including thinking, reasonable people, and key backup people, who can calmly work through a situation. Each and every situation is different. (NOTE: Copies of documents specified here can be requested).

Integration into University Planning

Disaster recovery planning occurs at multiple levels. First, the University has an emergency response plan that covers event identification, general policy, initial response, emergency notifications and communication, crisis management teams and communications. That document identifies emergency events for IT and we include IT events in that list (Document: Compromise of Information Technology Systems). This list is part of a Desktop Guide that has been distributed to all university employees to keep at their desk. This represents the central IT effort to communicate with the campus community about what an IT disaster can look like and what they need to do. We've learned that some "disaster" activities can go ignored because the event is not recognized as an IT disaster.

Necessary Background Work

Periodic risk review is required, preferably separated by facilities and non-facilities issues. Such periodic review should include a facilities walk-through by local fire inspectors, investigative review of all data-center facilities by a fire safety consultant, or review by an insurance provider. Campus police or public safety officials should review physical security of facilities. Periodic reviews should be conducted with the university's Risk Management staff and with Internal Audit staff. Network security audits are also important. The campus must have an idea of how purchasing, shipping and receiving can work from an off-campus location, and from paper.

Standard communications paths cannot be expected to work in a disaster. In any given disaster event, different communications work. Plan for multiple communications paths:

- Digital, analog, walkie-talkies and cell phones (all three) in critical locations: police, president's office, main datacenter, etc. Pagers and digital pagers are not reliable.
- Pre-designated meeting location and time known to core recovery team members.
- Integrate IT communications in a campus communication plan. One person should be designated to communicate with the off-campus community.

Priority of Application Recovery

We followed these steps to identify the initial priority, and we continue to do ongoing review based on these steps.

1. Scan network to identify all the server-based systems on the network.

2. Review server-based systems with different constituent groups: president's cabinet, academic computing committee, Banner operating committee, distributed technology support committee, academic and administrative councils, and any other interested group.
 - a. What is your workgroup's primary purpose or objective, especially in using these systems?
 - b. What is the worst thing that could happen?
 - c. What is the worst thing that has already happened?
 - d. What data do you use every day and where does it come from?
 - e. What critical output do you produce every day and where does it go?
 - f. When is system access most critical?
3. Based on the answers, rate each system simply: high, medium, low.
4. Aggregate the "highs" into a group, and verify that group dependencies are listed first, especially hidden systems that the constituent groups would not recognize as high priority, such as DHCP and DNS.
5. Establish a server shut-down order and a server start-up order.
6. Review the services run on the servers, in order, and create a subordinate service shut-down and start-up order.
7. Separate expectations about return to service into facility-intact and facility damaged disasters. Different responses are required. Establish a published facility-intact return to service schedule, based on agreement from campus leadership (typically 4-12 hours). Facility-damaged schedules differ; return to service schedules need to reflect insurance inspections of at least 48 hours, and a rebuild of the datacenter in another location can take longer. Return to service is directly related to the amount of funding invested in disaster recover in advance of an actual event. Campus leadership should be involved in the investment decision and the standards for return to service.

IT Documentation for Event Handling

Internally, central IT has a formal Disaster Recovery plan overview. Each central IT employee has a handbook to use to evaluate specific systems and events (Document: Handbook).

The full plan is available to team leaders and is stored in a safe deposit box off site for retrieval. It consists of the following documents:

- Disaster Recovery Plan Overview
- Operational Handbook
- Server Shutdown/Restore Order with Location
- Asset Report
- Server architecture / Interface diagram
- Network Topology diagram
- Network outage management process
- Network event problem classification
- Network demarcation equipment diagram
- Contact info: home, office and cell phone info for all of the IT staff
- Home, office and cell phone info for key campus decision makers

Contact and contract information for support vendors

Data backups are stored at an off-site location, and a backup library listing is maintained. A copy of the emergency document library is kept in an off-campus safe deposit box, paper copy to enable the fastest readable access. Everything needed to run the datacenter, including a copy of all needed forms, is kept off-site.

University Technology Services Disaster Recovery Plan

March 4, 2004

Introduction

The University Technology Services Disaster Recovery Plan follows, and is considered part of, the larger Oakland University Emergency Response Plan. Under that plan, an emergency event will be identified and verified through standard and documented university procedures and a response effort will be triggered as a result. The response will be communicated through the Critical Incident Communications Management Plan. Once the communication has been received in University Technology Services, UTS staff will implement the procedures in the University Technology Services Operational Handbook.

Based on the environment we have built, as described above, our goal is to return normal services in less than twelve hours, as long as there has not been damage to major facilities or equipment (particularly the Key-Building Data Center). A facility intact disaster can be controlled through the systems planning, redundancy and security that we have built into our environment. A damaged facility requires different action and scheduled replacement of facilities or equipment may proceed after an initial 48 hours for insurance documentation and assessment. The decision to move to the alternative facility will be made under existing University Emergency Response Plan procedures.

Plan Activation

An emergency will be determined under the Emergency Response Plan and notification will be received under the Critical Incident Communications Management Plan. The University Technology Services Operational Handbook procedures will be followed. If a *Critical Systems Emergency* is initiated, as defined in the Handbook, this University Technology Services Disaster Recovery Plan will be initiated by the convening of the Disaster Recovery Team. The Assistant Vice President of University Technology Services, or a designee defined by the Crisis Management Team (under the Emergency Response Plan), will convene the Disaster Recovery Team.

Disaster Recovery Team

The Disaster Recovery Team will be assembled and apprised of the damage to resources and facilities. This group will represent University Technology Services in university efforts to recover from a disaster. Members of the Disaster Recover Team will include the following individuals. Others will be involved in the process as needed.

- Assistant Vice President
- Director Operations
- Manager Operations
- Database Applications Team Leader
- Technical Support Team Leader
- Network Communications Team Leader
- Security and Helpdesk Manager

Plan of Action

The UTS Disaster Recovery Team will:

1. Establish a reasonably located command central for the Team. If possible 218 Key-Building Hall will be used. If not possible, contact the Assistant Vice President or the designee defined by the Crisis Management Team for location.
2. Assign senior staff member to be the single point of contact with the Crisis Management Team.
3. Designate one member of the Disaster Recovery Team as “public relations representative” for this purpose at the time of the incident. The designated team member will handle all associated UTS communications, and make frequent and ongoing statements of status to Communications and Marketing.
4. Retrieve backup tapes and documentation materials from on-campus or off-campus storage as needed. Contact vendor at xxx-xxxx. Essential to this step is the retrieval of the archived Fixed Assets database. The team will designate a “retrieval representative” for the purpose of retrieving any off-site restoration materials.
5. Distribute short-wave radios or cell phones for communications.
6. Coordinate and make decisions.
7. Lead technical effort to restore systems and communications to operation.
8. Assess hardware operability or lead purchasing efforts to replace hardware.
9. Analyze minimum processing needs.
 - A. Assess ability to meet payroll and report to the Crisis Management Team.
 - B. Assess ability to meet instructional information technology needs and report to the Crisis Management Team.
10. Establish priorities and scheduling requirements.
11. Review the Data Center site and other UTS facilities, and assess damage, making a joint decision with the representatives of the Crisis Management Team as to whether the facility is intact or whether an alternative facility must be activated.
12. Coordinate clean up or relocation activities.
13. Report on financial aspects of disaster.
14. Alert vendors and contractual relationship contacts. Working with the Finance division, verify that vendors RETIREMENT, BANK and other vendors are notified as needed.
15. Conduct an annual review of this plan, and a post-disaster review of this plan.

Efforts will focus on verification and restoration of tier one systems, in restore order as defined on the Fixed Assets database:

1. Telecom plant
 - a. Verify operation of telecom / network demarcation environment in North Building Hall: fire suppression, air conditioning and electrical service with uninterruptible power supply.
 - b. Verify operation of main Telecom-Vendor switch. The switch should return to operation automatically and immediately after return of electrical service. Check both delivery and receipt of on-campus and off-campus calls, and 911 service. Telecom-Vendor emergency contact is xxx-xxxx press 1 → 1 to report a major outage. Account number is xxxxxxxx for Product xxx/99.
 - c. Verify operation of PhoneMail voice mail, 911 service, alarms and other critical telecom services.
 - d. Verify Key-East-Building House phones by calling xxx-xxxx from on and off-campus. If the phone goes to a standard message or is answered, service is restored. If there's no answer, ongoing ringing, etc., we proceed to verify by calling University Relations phone tree to ask for a review of alarms on the console. If we cannot get University Relations contacts, or if the alarm cannot clear, proceed to call vendor at xxx-xxxx.
 - e. Contact Communications and Marketing to update University phone messages.
 - f. Notify Public Safety on telephone operations status.
2. Key-Building Data Center Facility air conditioning and electrical service with uninterruptible power supply
 - a. Verify UPS operation. Vendor contact xxxxxxxx.
3. Core router, switch units and network support systems
 - a. Contact contracted network support vendor at xxxxxxxx.
4. Restoration of network systems that support physical plant operations

- a. Verify power to Key-Building Datacenter network rack.
 - b. Verify network operations in network demarcation.
 - c. Verify operation of network demarcation environment: air conditioning and electrical service with uninterruptible power supply.
 - d. Verify network connectivity to Central Heating Plant and contact CHP on return of service. Contact CHP – xxxx.
 - e. Verify network operations.
5. Restore systems in Operations systems order (reverse mirror of shut-down order).
- a. DNS / DHCP / WINS servers and the domain controllers
 - b. Authentication / authorization
 - c. University Technology Services staff desktop or laptop computers
 - d. Internet service provision
 - i. Verify Merit connectivity www.merit.edu
 - e. Backup systems
 - f. Email services
 - g. Trouble-ticketing systems
 - h. File storage services
 - i. Basic administrative Banner environment: production database server, Banner forms server cluster
 - i. Payroll processing systems verification
 - j. Online learning WebCT server environment
 - k. General print services
 - l. Banner Web-For and Touchnet environment
 - m. Verify remote systems through Distributed Technology Support group and XXX Law School
 - i. Library
 - ii. Student ID card
 - iii. Golf course
 - iv. Special facilities