Payoff

The true test of a disaster recovery plan is whether it can uncover failure points. Companies should consistently tighten testing criteria and review test results to ensure that a disaster recovery plan executes under a variety of conditions. A checklist of issues and errors tailored to specific disaster recovery teams aids in refining the test process.

Introduction

Determining the effectiveness of a disaster recovery plan, or whether a plan works at all, is as crucial to the plan's development as the documentation of operating and security standards and recovery procedures. This article presents checklists of issues and errors that often occur during disaster recovery tests. It is based on an exercise conducted by a large fictitious company whose Executive Management Team works in coordination with other logistical teams to oversee a highly visible disaster. Reviewing the functioning of these varied teams can help other IS managers develop or refine a test and ensure a more cohesive recovery exercise for their organizations.

The Executive Management Team

At a minimum, an Executive Management Team should comprise a chief executive, a director of technical services, a building facilities manager, and a small administrative staff. It is called together only under specific circumstances, such as a destructive disaster that necessitates moving the company's primary place of business to a disaster recovery facility; an environmental disaster, such as a hazardous chemical spill, that poses a complicated public affairs problem; or a disaster that is considered a threat to investors, shareholders, or customers who depend on the organization and require a high level of public contact and reassurance. The primary requirement of an executive management team (EMT) is a predefined location—such as a training facility, hotel suite, or one of the executive's homes—to which the executives know to report after a disaster.

Activating the EMT

Successful activation of an executive management team (EMT) depends foremost on the ability to contact team members during the difficult and unusual circumstances a disaster poses. Several basic issues can arise during the notification process: Do key executives have unlisted telephone numbers that are not documented in the plan? Even if they do not, what if telephone service is out to the area? Do they have a backup, such as a pager or a cellular phone?

Contacting employees at their homes regarding disasters at the facility involves other more subtle issues. For example, what if an employee was at the facility when the disaster occurred? People making the calls to employee homes should be prepared to deal with hysterical relatives who may be hearing for the first time that a disaster has occurred at the facility where a loved one works. Providing a preapproved checklist that contains not only names and telephone numbers but also a brief procedure to follow when contacting employees' families can help circumvent these problems.
Once notified, the correct executive management team (EMT) members should assemble at the predetermined location or command center. Under already difficult conditions, executive management team (EMT) members may have trouble following directions to the command center. Planners should choose a location that is central enough for easy reach by team members. These issues can be mitigated in large part by establishing the command center at a landmark that has ready access to telephone service.

**Operating the Command Center**

The executive management team (EMT) needs to be able to begin work on arriving at the center. Several items must be immediately available to the executive management team (EMT), such as telephones, fax machines, a small copier perhaps, and, although less apparent, a place to sit. Documenting the command center's setup allows technical personnel to ensure that the center can begin operations promptly.

To prevent executive management team (EMT) members from wasting precious time trying to figure out how to use emergency telephones, a basic touchtone analog telephone set should be used. Workers should be able to plug in a fax, laptop machine, or modem to the telephone as well.

The executive management team (EMT) must receive critical status and damage reports in the time frame prescribed in the recovery plan. A successfully activated executive management team (EMT) works with several logistical teams involved in the technical aspects of the recovery process. Once notified of the disaster, the teams fan out citywide or perhaps nationwide to implement the company's recovery plan. One team is dispatched to the disaster recovery center, if one is in use; another is dispatched to the affected facility to aid in restoration; and still more teams travel to perform such functions as retrieving stored magnetic media and picking up and delivering equipment.

**Refining the Test Process**

The importance of testing disaster recovery plans must be communicated, as well as the ability of even the most advanced organizations to learn something each time they test their recovery plan. To strengthen their company's plan, team members should make notes during and after the test. For effective updating, the plan and test procedures should be reviewed immediately following any test and activation, when memory is fresh. Executive Management Team members can learn lessons from the exercise, including what procedures they would change next time they test the plan. For example, executive management team (EMT) members may feel that recovery could have been facilitated by the representation of other areas in the company on the team, such as the real estate department and human resources.

**Technical Service Teams**

Many organizations use commercial off-site disaster recovery facilities from a variety of sources. While these sources specialize in recovery, they cannot do the job alone. Several teams of technical service personnel must be mobilized to staff and configure a recovery center. Some of the most basic are suggested here.

Despite the trend toward distributed processing, mainframes are still used by many companies. The team responsible for what is generally the oldest but still core component in many recovery plans must be activated.
Mainframes, however, are only one component of a business and its recovery plan. Today a mainframe supports many functions that it did not support in the past. One of these things, of course, is LANs. Restoring LANs means more than restoring a server and wiring. To effectively restore a LAN business function, the three components of a business recovery solution are needed:

- An attendant position.
- The data that resided on the LAN.
- The communications link that turns the employees using the LAN into revenue generators for the company. These links will play a prominent role in recovering LANs, both for voice and data communications.

Other teams involved in the recovery include field services teams comprising personnel who may normally support personal computers or terminals from a maintenance standpoint and can serve as emergency installation technicians for the new configurations. Various engineering teams, or teams of senior analysts, may also be involved to provide high-level trouble-shooting and support when complex equipment configurations must be literally built overnight.

**Mobilizing Technical Service Teams**

Mobilizing technical service personnel involves many of the same issues as mobilizing the Executive Management Team. For instance, team members obviously will need easy-to-follow directions to the recovery center. Planners, however, must address additional factors. In cases of widespread disasters, as many as 50% of employees will go home to check on their homes and families before reporting to work. It is therefore imperative to test how the recovery plan would work in the absence of key technical personnel. Removing a few personnel in a simulation effectively tests how others will compensate.

**Setting Up the Recovery Center**

Commercial disaster recovery centers are shared by many organizations. A company must be aware that its site probably was used by others between tests and that configurations most likely were changed.

Personnel unfamiliar with a company's day-to-day environment will rely on diagrams and a documented recovery plan to set up equipment. The company's key technical people will know where equipment goes and how to set it up, but there is no guarantee they will be available during a disaster. Even when company personnel are present, they will be installing overnight what originally took years to create. Equipment service or installation manuals should be readily at hand in the event they are needed. Similarly, commercial recovery sources must provide on-site guides to demonstrate the subleties of equipment used at the center, such as complex matrix switches.

**Restoring Communications**

Technical service teams must deliver a report to the executive management team (EMT) within a prescribed time frame. Restoring communications is therefore one of the
teams’ priorities. If the recovery center does not provide regular touchtone analog telephones, personnel should be trained in advanced on the telephones at the center.

Efficient restoration of communications involves several tasks. When a large amount of technical equipment must be installed in a short time, keeping the same help desk or network control number enables vendors supporting the recovery process to contact a company easily, avoiding unnecessary delays. Dial-in data, switched digital service, and Integrated Services Digital Network links must also be successfully established.

The complement of telecommunications services that support data transmission for users must be checked in advance. One common problem with T1 links, for example, concerns the fact that most T1 local loops to recovery centers are shared among a broad user community. Because each customer using these links may be using a different line code for the T1, the links may have been reoptioned since a company's last disaster test and may not work without modification.

Procedures for reoptioning Channel Service Unit (CSUs) and other components that may have changed should be detailed in the recovery plan. The best test in all of these cases is a live test. Even if live production data is not transmitted, running a test pattern across these facilities can ensure that the telecommunications facilities are in tact, work properly, and would support data if necessary.

Data Delivery and Restoration

Data stored off-site must be delivered to the recovery center for such components as the mainframe and LAN; telecommunications, switches, and multiplexers; the voice mail system; and automated call distribution (ACD) units. Procedures for retrieving mainframe and LAN data, which are typically stored off-site, are already in place. With coordination, telecommunications data may also be picked up during this procedure.

Problems in removing software from one system and reinstalling it on another stem from subtleties in operating systems or even minute differences in components such as tape drives. Although this problem is common, shortcuts that facilitate a more graceful reload on the new systems can be learned.

Evaluating Performance

Like members of the executive management team (EMT), technical personnel should document what they learned from the exercise and what should be changed for the next test. Some of the issues requiring documentation are basic, such as whether the test equipment installed at the center for general use was surveyed in advance, appropriate for the company's test processes, and functioning properly. Even seemingly insignificant items, such as hand tools, should have been available and adequate. It is also highly recommended to request of principal equipment vendors that a representative be present at the recovery center, and to rate each vendor's response to the request.

No team can accomplish its goals without an overall environment reasonably conducive to the company's work environment. This issue is especially important in cases of distributed processing. While ergonomics may be a problem and people may be working on folding tables, the recovery assembly should help everyone get the job done. If not, team members should specify what is needed to bring the recovery center up to par.

Successful performance of tasks also depends on effective use of personnel at a time when personnel are at a premium. Team members should evaluate whether representatives of other areas of the organization would have facilitated work at the recovery center. Or, stated another way, they should ask whether an area was unnecessarily represented at the
center. Someone who may be a fifth wheel at the recovery center could be reassigned to assist in restoring the damaged facility, for example.

Thorough documentation also includes communicating to management that the true test of a plan is whether it can uncover failure points. Consistent flawless results on recovery tests indicate that an organization should tighten its standards.

The Facility Reconstruction Team

The facility reconstruction team comprises a complement of personnel who are dispatched to the damaged site to survey conditions, report to the Executive Management Team, and coordinate with local and emergency authorities. The team could include members of the company's building services group and representatives of the production, LAN, mainframe, telecommunications, or other divisions that have a high content of equipment in the building. Other teams, such as administrative or logistical supply teams, should also be considered, as well as a media affairs representative.

Again, testing criteria for the facility reconstruction team are similar to those discussed previously, with notable exceptions. A checklist for the reconstruction team follows.

Restoring the Damaged Facility

The Right People for the Job. Only employees required for the recovery process should assemble at the site after a disaster. Others who report to satisfy their curiosity may interfere with the recovery process, especially by tying up valuable cellular telephone frequencies with personal or unnecessary calls.

The specific complement of personnel who report to the damaged site depends on the type of disaster that has occurred. In the case of a fire, the building facilities manager should be present to interface with local emergency personnel who control the facility until it is deemed safe for entry. A knowledgeable building facilities manager could help these personnel decide issues more quickly. Similarly, in cases of a highly visible or widely broadcast disaster, a media affairs representative is needed to interact with the inevitable high volume of media presence. In almost all disasters, it is a good idea to have at least one security person on the team to assess the situation and determine whether additional security reinforcements are required to secure the building from theft.

A smoothly functioning reconstruction team also depends on clearly delineated responsibilities. Without them, conflicts or turf issues may develop over such issues as which department is responsible for rewiring the building. There are probably five different people in the organization (from facilities, LAN management, telecommunications, and other departments) who will believe themselves responsible for rewiring, so predefined responsibilities will avoid overlap, wasted efforts, and squabbles during the recovery.

Adequate communication among members is also a must. Team members should feel like a cohesive unit during the test. If they frequently feel out of touch with others, communications must be improved to foster cohesiveness.

Appropriate Equipment.

Each member of the team that enters what may be a severely damaged facility needs certain standard equipment, such as a flashlight with a spare set of batteries; a hard hat; an identifying badge or, preferably, an identifying vest to quickly differentiate between employees and looters; a copy of the recovery plan; a small notebook to annotate critical events and document important command decisions made during the recovery process;
and at least one roll of quarters in the event that a major telecommunication disaster renders other services unavailable or overwhelmed. The team should also have at least two cellular telephones, two two-way radios, two pagers to keep track of people on-site and expedite the recovery process, and at least one cellular fax and a laptop computer with a fax modem card to aid in reporting to the executive management team (EMT) in the prescribed time frame.

A Staging Area for Recovery Operations.

When a building is totally inaccessible or lacks the required telecommunications, water, or sanitary facilities, facility reconstruction personnel should promptly report to a prearranged staging area for recovery operations, such as in a nearby hotel. Telephone numbers must be promptly diverted to the staging area. The network control number may be diverted to the recovery center, for example, for technical questions regarding mainframes or LANs. The help desk number, however, may be diverted to the staging area.

Notifying Professional Clean-Up Personnel.

Professional clean-up companies have the answers to such questions as what to do with magnetic tapes that have been wet in a disaster (they should be put in the freezer). The companies use a freeze-dry process to save valuable data stored on magnetic media and similar processes for wet paper and smoke-damaged equipment. Immediate notification is crucial, since the processes must be performed within the first 48 hours following a disaster.

Evaluating and Documenting Test Results

Facility reconstruction personnel must evaluate similar issues as their colleagues on the executive management team (EMT) and technical service teams. Most important is whether an initial status report was dispatched to the executive management team (EMT) within the 90 minutes specified in most disaster recovery plans. Other issues include whether equipment was adequate, whether on-site vendor representatives were immediately summoned and current telephone numbers listed for them, whether the complement of team members was effective, and what should be changed for the next exercise.

Conclusion

The teams involved in a disaster recovery test have different tasks, goals, and needs, yet the testing procedure holds the same overriding message for all of them: Testing a plan is a learning experience. Organizations should not expect their first test to run perfectly, nor aim for perfect results each time they test. Testing until failure makes for a true test.

Once testing procedures become routine, criteria should be tightened, or key personnel removed from the process to ensure that the plan executes in a variety of circumstances. Successful testing of a plan provides greater peace of mind and assures management that the time and money spent in developing and honing the test was a wise investment.

Author Biographies

Leo A. Wrobel is president of Premier Network Services Inc., in Dallas.