TechRepublic Resource Guide

Disaster Planning and Recovery

Contents

Develop an effective disaster recovery plan

By Rick Schiesser

During the mid- and late 1990s, I managed the main IT infrastructure for a major motion picture studio in Beverly Hills, California. Just prior to my hiring, an event drastically changed the corporation's thinking about disaster recovery, and I was asked to develop a disaster recovery program of major proportions.
Two of this studio's most critical applications were just coming online and were being run on IBM AS/400 midrange processors. One of the applications involved the scheduling of broadcast times for programs and commercials for the company's new premier cable television channel. The other application managed the production, distribution, and accounting of domestic entertainment videos, laser discs, and interactive games. The company had recently migrated the development and production versions of these applications onto two more advanced models of the IBM AS/400—9406-level machines utilizing reduced instruction set computing (RISC) technology.

During the development of these applications, we began initial discussions about developing a disaster recovery plan for these AS/400s and their critical applications. In February 1995, the effort got a major jumpstart from an unlikely source. A distribution transformer that powered the AS/400 computer room from outside the building short-circuited and exploded. The damage was so extensive that repairs were estimated to take up to five days. With no formal recovery plan yet in place, IT personnel, suppliers, and customers all scurried to minimize the impact of the outage.

With the help of one of the company's key vendors, we quickly identified and activated a makeshift disaster recovery site located 40 miles away. Within 24 hours, the studio's AS/400 operating systems, application software, and databases were all restored and operational. This makeshift solution met most of the critical needs of the AS/400 customers during the six days that it eventually took to replace the failed transformer.

Three important lessons learned

This incident accelerated the development of a formal disaster recovery plan. It also underscored three important points about recovering from a disaster. The first point is that there are noteworthy differences between the concept of disaster recovery and that of business resumption. I'm defining business resumption as the ability to perform critical department processes as soon as possible after the initial outage. Full recovery from the disaster usually occurs many days after the start of the business resumption process.

In this case, we restored most of the company operations affected by the outage in less than a day after the transformer exploded. It took nearly four days to replace all the damaged electrical equipment and another two days to restore operations back to their normal state. Distinguishing between these two concepts helped during the planning process for the formal disaster recovery program—it let us focus on business resumption in meetings with key customers, while we focused on disaster recovery with key suppliers.

The second point is that most computer center outages are caused by relatively small, localized incidents like broken water mains, fires, smoke damage, or electrical equipment failures—not the flash floods, powerful hurricanes, or devastating earthquakes frequently highlighted in the media.
This isn't to say that you shouldn't be prepared for such a major disaster. Infrastructures that plan and test recovery strategies for smaller incidents are usually well on their way to developing a program to handle any size of calamity. While major calamities do occur, they are far less likely and are often

overshadowed by the more widespread effects of the disaster on the community. What usually makes a localized computer center disaster so challenging is that the rest of the company is normally operational and desperately in need of the computer center services that have been disrupted.

The third point is that this extended outage prompted executive management to make a firm commitment to a formal disaster recovery plan. In many ways disaster recovery is like an insurance policy: You don't really need it until you really need it. This commitment was the first important step toward developing an effective disaster recovery process. A comprehensive program requires hardware, software, budget, and the time and efforts of knowledgeable personnel. The support of executive management is necessary to make these resources available.

Steps to developing an effective disaster recovery process

There are 10 steps to developing an effective disaster recovery process:

1. Obtain executive support.

Executive support, particularly in the form of an executive sponsor, is necessary for developing a truly robust disaster recovery process. You need funding approval from senior management for the resources you need in order to design and maintain an effective disaster recovery program.

Another reason this support is important is that managers are typically the first to be notified when a disaster occurs. This sets off a chain of events involving management decisions about deploying the IT recovery team, declaring an emergency to the disaster recovery service provider, notifying facilities and physical security, and taking whatever emergency preparedness actions may be necessary. By involving management early in the design process, you secure their emotional and financial buy-in, thus increasing the likelihood that management will understand and fulfill its role in the disaster recovery process.

The executive sponsor has several other responsibilities. One is selecting a process owner. Another is getting the support of other managers to ensure that participants are properly chosen and committed to the program. These other managers may be direct reports, peers within IT, or, in the case of facilities, outside of IT. Finally, the executive sponsor needs to demonstrate ongoing support by requesting and reviewing frequent progress reports, offering suggestions for improvement, questioning unclear elements of the plan, and resolving issues of conflict.

2. Select a process owner.

The process owner is the most important person in the disaster recovery process because of the many key roles he or she plays. The process owner must assemble and lead the cross-functional team in preparing the business impact analysis, identifying and prioritizing requirements, developing business continuity strategies, selecting an outside service provider, and conducting realistic tests of the process. The process owner should exhibit several key attributes and be selected very carefully. Potential candidates include an operations supervisor, the data center manager, and even the infrastructure manager.

3. Assemble a cross-functional team.

The process owner must assemble representatives from appropriate departments into a cross-functional design team. Departments typically represented on this team include computer operations, applications development, server and systems administration, facilities, key customer departments, data security, physical security, and network operations. This team will work on requirements, conduct a business impact analysis, select an outside service provider, design the final overall recovery process, identify members of the recovery team, conduct tests of the recovery process, and document the plan.

4. Conduct a business impact analysis.

Even the most thorough disaster recovery plan won't be able to justify the expense of including every business process and application in the recovery. It's important to inventory and prioritize critical business processes for the entire company. Key IT customers should help the process owner coordinate this effort to ensure that all critical processes are included. Processes that need to be resumed within 24 hours to prevent serious business impact, such as loss of revenue or major impact to customers, are rated as an A priority. Those processes that need to be resumed within 72 hours are rated as a B, and those that can take more than 72 hours are rated C. These identifications and prioritizations will be used to propose business continuity strategies.

5. Identify and prioritize requirements.

One of the cross-functional team's first activities is to identify the requirements for each process, such as business, technical, and logistical requirements. Business requirements include defining the specific criteria for declaring a disaster and determining which processes are to be recovered and in what time frames. Technical requirements include what type of platforms will be eligible as recovery devices for servers, disks, and desktops, and how much bandwidth will be needed. Logistical requirements include the amount of time allowed to declare a disaster and transportation arrangements at both the disaster site and the recovery site.

6. Assess possible business continuity strategies.

Based on the business impact analysis and the list of prioritized requirements, the cross-functional team should propose and assess several alternative business continuity strategies. These will likely include alternative remote sites within the company and geographic hot sites supplied by an outside provider.

7. Choose participants and clarify their roles for the recovery team.

The cross-functional team chooses the individuals who will participate in the recovery activities after any declared disaster. The recovery team may be similar to the cross-functional team but should not be identical. Additional members should include the executive sponsor, key customer representatives, and representatives from any outside service providers. Once the recovery team is selected, it's imperative that each individual's role and responsibility be clearly defined, documented, and communicated.

8. Document the disaster recovery plan.

The last official activity of the cross-functional team is to document the disaster recovery plan for use by the recovery team, which will then have responsibility for maintaining its accuracy, accessibility, and

distribution. Documentation of the plan must also include up-to-date configuration diagrams of the hardware, software, and network components involved in the recovery.

9. Plan and execute regularly scheduled tests of the plan.

Disaster recovery plans should be tested a minimum of once a year. Progressive companies test three or four times annually. Maintain a checklist during the test to record the disposition and duration of every task, and compare it to the list of planned tasks. Consider developing a test plan that spans up to three years—every six months the tests can become progressively more involved, starting with program and data restores and followed by processing loads and print tests, then initial network connectivity tests, and eventually full network and desktop load and functionality tests.

10. Conduct a lessons-learned postmortem after each test.

The intent of the lessons-learned postmortem is to review exactly how the test was executed as well as to identify what went well, what needs to be improved, and what enhancements or efficiencies could be added to improve future tests.

Nightmare incidents

During many years of managing and consulting on IT infrastructures, I've encountered a number of nightmarish disaster recovery incidents. Some are humorous, some are "head-scratching," and some are just plain bizarre. In all cases, they totally undermined what would have been a successful recovery from either a real or simulated disaster. Fortunately, no single client or employer with whom I was associated ever experienced more than any two of these, but in their eyes, even one was unacceptable. These incidents, listed below, illustrate how critical planning, preparation, and performance are to a good disaster recovery:

- Backup tapes have no data on them.
- Restore process has never been tested.
- Restore tapes are mislabeled.
- Restore tapes can't be found.
- Offsite tape supplier hasn't been paid and can't retrieve tapes.
- Graveyard-shift operator doesn't know how to contact recovery service.
- Recovery service to a classified defense program is not cleared.
- Recovery service to a classified defense program is cleared, but individual personnel aren't cleared.
- Operator can't carry tape canister onto the airplane.
- Tape canisters are mislabeled.

The first four incidents all involve the handling of the backup tapes required to restore copies of data rendered inaccessible or damaged by a disaster. Verifying that the backup and, more importantly, the restore process are completing successfully should be one of the first requirements of any disaster recovery program. While most shops verify the backup portion of the process, more than a handful of

shops don't test to verify that the restore process also works. Labels and locations can also cause problems when tapes are marked or stored improperly.

Although a rare case, I do know of a client who was unable to retrieve a tape because the offsite tape storage supplier hadn't been paid in months. Fortunately, it was not during a critical recovery. Communication to, documentation of, and training of all shifts on the proper recovery procedures are critical. Third-shift graveyard operators often receive the least of these due to their off hours and higher-than-normal turnover. These operators need to know whom to call and how to contact offsite recovery services.

Classified environments can present their own brand of recovery nightmares. One of our classified clients had applied for a security clearance for its offsite tape storage supplier and had begun using the service prior to the clearance being granted. When the client's military customer found out, the tapes were confiscated. In a related issue, a separate defense contractor cleared its offsite vendor to a secured program but failed to clear the one individual who worked nights when a tape was requested for retrieval. The unclassified worker couldn't retrieve the classified tape that night, delaying the restoration of the data for at least a day.

The last two incidents involve tape canisters used during a full dry-run test of restoring and running critical applications at a remote hot site 3,000 miles away. The airline in question had just changed its carry-on baggage policy, which meant the recovery team couldn't keep the tape canisters with them. Making matters worse was the fact that the canisters were mislabeled, which cost over six hours of restore time. There was much to talk about during the marathon postmortem session that followed this incident.

10 things you should cover in your business continuity plan

By Debra Littlejohn Shinder, MCSE, MVP

1. Analysis of potential threats

Your company's response to a disaster will depend on both the nature and the extent of the disaster. Some threats, such as a tornado or flood, may physically destroy your IT infrastructure. Others, such as pandemic disease, affect human resources while leaving buildings and machinery intact. A cyberterrorism attack might bring down your network but not affect the functionality of the hardware or your personnel. A bombing may destroy both human life and network components. A power outage could render your equipment unusable, but do no lasting damage. Thus your plan should cover contingencies for as many threat types as possible.

2. Areas of responsibility

A key component in any crisis management situation—which is what you have during and perhaps immediately after the disaster—is assignment of areas of responsibility and establishment of a chain of command. This is no time to have department heads squabbling about who has decision-making authority. And remember that some types of disasters may result in loss of personnel (or some of your staff may be on vacation or out sick when the event occurs), so be sure to assign alternates in case some of the important players are not available.

Training of key personnel in disaster preparedness, incident management, and recovery should also be addressed.

3. Emergency contact information

Your plan should include up-to-date contact information on people and entities that may need to be contacted when a disaster occurred. This is no time to be scrambling for phone numbers. Information should be included for both internal personnel (CEO, CIO, legal advisor, etc.) and external personnel and services (police, fire, ambulance, security services, utility companies, building maintenance, etc.).

4. Recovery teams

It will take teamwork to manage the crisis itself and to put things back together once the immediate crisis is over. The BCP should appoint members of a disaster recovery team (DRT) made up of specialists with training and knowledge to handle various aspects of common disasters (safety specialist, IT specialist, communications specialist, security specialist, personnel specialist, etc.). The DRT members will work with emergency services during the disaster and should have access to equipment they'll need during an emergency (cell phones, flash lights, hard hats, protective clothing, etc.).

A business recovery team is responsible for reestablishment of normal operations after the crisis is over.

5. Off-site backup of important data

Any good business continuity plan will address restoration of your company's important digital data if it is destroyed. Too many organizations meticulously make backups of everything and then store those backups in the server room. If a tornado, flood, or bomb destroys the building, that (often irreplaceable) data is gone, too.

You should store copies of important data on removable media that's kept at a different physical location or back it up over the Internet to a remote server, or both. Just as important, key personnel should know where it's stored and have the keys, passwords, etc., to be able to restore it to get users back to a productive state as soon as possible.

6. Backup power arrangements

Many types of physical disasters can result in a loss of electrical power, or a power outage can, itself, be the disaster. For continuity of business, your organization should plan for what to do in case of a long-term outage (more than the hour or less that your uninterruptible power supplies will keep your computers and network equipment running).

If you have backup generators in place, ensure that key personnel know how to switch to generator power and know the fuel requirements for the generators (must they be fueled or do they run off the natural gas line?), among other practical issues. Consider cost factors to determine when and for how long the generators should be run. Providing full electrical power to a building with a generator can cost much more than using the power grid, so the BCP should discuss in what situations it's better to close down operations and send everyone home rather than run on generator power, and it should define who has the authority to make that decision.

7. Alternative communications strategy

If your company's phones and/or Internet connection are down, how will you keep in touch with customers, employees who are off-site, contact emergency services, etc.? Your BCP should note which employees have cell phones and their numbers, as well as whether and where you have other methods of communicating during a widespread disaster, such as ham radios. If you run your own e-mail servers, do key employees have alternative e-mail addresses that they check regularly (home accounts or accounts with Web-based e-mail services, etc.) and are these addresses known to other key personnel in case they're needed for emergency contact?

8. Alternative site of operations

The BCP should also spell out a plan for setting up operations at an alternative location if the building is destroyed or rendered unusable by a disaster. Best practice is to have ready access to an empty facility that you can move into; a more practical (less expensive) alternative would be to move your operations to a branch office if you have more than one physical site.

The BCP should also take into consideration the estimated costs of moving, setup, and ongoing operations in the new facility.

9. Essential equipment/services backup

In some cases, you may be able to recover essential equipment and move it to a new site. In others, it may be destroyed or damaged and have to be replaced or repaired. The BCP should lay out how the equipment or its functions will be replaced (for instance, you may switch to a Web hosting or e-mail hosting service until you're able to replace your servers and get them operational again).

10. Recovery phase

The BCP should address the step-by-step process of recovering and reinstating the business operations to a pre-disaster state, including assessing the damage, estimating recovery costs, working with insurance companies, monitoring the progress of the recovery process, and transitioning the management of the business operations from the recovery team back to the regular managers.

10 items for your disaster recovery wish list

By Rick Vanover

We all have to address disaster recovery (DR) at various levels, but we typically must apply the technology to fit rigid parameters—such as less cost or functionality—instead of being able to do it right. But what if you didn't have any limitations to hold you back? How would you create the perfect DR model? Here are some things (however unrealistic) that might go into building the perfect environment for meeting DR requirements.

1. The network is transparent

Providing transparent network connectivity is our number one challenge in making the ideal DR environment. If subnets for data center components were designed to be available across multiple locations without reliance on one piece in another data center, DR failover would be a breeze. Sure, a lot can be done to manage the use of a DR site through DNS and virtual switches—but if those could be avoided for a more natural configuration, the process could be made easier and work in a more transparent fashion.

2. The storage is transparent

Storage could arguably take the #1 spot on our list, since it's such a big pain in DR configurations. Technologies are available to handle storage replication and set up storage grids, but how many of us have the money to implement the functionality? The ideal DR storage system would also dispel any performance limitations when you're running the entire enterprise from the DR configuration. Limitations in performance may cause a selective DR, which makes for difficult decisions on what systems are truly required in the DR environment.

3. Everything starts with DR in mind

How many times have you come across a system that began as a pilot or simple test, was promoted to a live role, and is singular in nature and can't scale? These are DR plan inhibitors. If all systems are designed with the DR concepts in mind, all systems can comply with the same DR requirements and be an easy transition for administrators.

This extends to the peripheral components as well—storage, data recovery, networking, and access to the system should be created with DR in mind. But too many times, a system may have some but not all of the DR components in place. "Mostly compliant" with the DR model is still noncompliant.

4. All areas of IT meet the same requirements

Have you ever been irritated by partial compliance with an enterprise DR policy? An example would be when one application meets a different standard of DR—so maybe only a few clients can run the application in the DR configuration. Wouldn't it be great if the standing policy for the organization was

to have full compatibility for the DR configuration? The ideal DR policy would provide funding and enforce the requirements for the DR configuration across all systems and groups within IT.

5. Disaster recovery is performed in a few steps

How we get to a solid and robust DR configuration will vary widely by size and scope, but the perfect conversion to the DR would a quick and contained process that is identified in a few steps per system, or a few steps for the entire environment. With the DR configuration so accessible, this would also be a good opportunity to enforce regular intervals where the DR configuration is used.

6. Documentation for failover to the DR site is clear and simple

An overly complex procedure to use a DR site can ruin the usability of the mechanism. The ideal DR environment has consistent and clear documentation that is practiced regularly so there's no guessing in switching to the DR model. In fact, regular use of the DR model can ensure that the remote DR site works as expected, keeps staff familiar with the procedure, and extends the life of primary systems by increasing idle time at the primary site.

7. All data recovery is native

The most challenging part of DR is the data recovery process. If a data recovery model is patched together using various scripts, watchdog programs, or other solutions that are not native to a product's feature set, the risk of data corruption and DR failure goes up. The ideal DR model would have solutions built into the product that consider all parts of a solution, as many products use more than just a database to provide the overall application.

8. Performance in the DR model isn't compromised

A comprehensive DR plan that meets all requirements from a design perspective yet can't handle the load is worthless. You don't want to have to decide which applications and systems are available at the DR site when you're in a DR situation. Limitations such as Internet connectivity, network bandwidth, shared storage throughput, backup mechanism availability, and storage capacity are all factors in gauging the overall performance for the DR site.

The perfect DR situation would be an exact inventory in the remote data center that models that of the primary data center. However, maintaining an equipment inventory in lockstep with another data center is nearly impossible. So the next-best solution would be a remote data center that meets or exceeds a performance benchmark set by the primary data center in all relevant categories.

9. The user experience in the change-over is nothing more than a reboot (if that)

Managing the transition to the remote data center is difficult enough on the data center. But the user side of the transition should be made as seamless as possible. Strong DR plans and mechanisms frequently base technology on DNS names (especially CNAME records) that can be easily switched to

reflect a new authoritative source for the business service. This can include standby application servers and mirrored database servers, as well as migration to new versions with the simple DNS change.

Managing the refresh or the caching of the names can be a little tricky, but either having clients reboot or run the ipconfig /flushdns command on Windows clients can usually refresh any caching. The same goes for server systems that are affected by a DR transition; they may need to refresh their own DNS cache, so the same configuration steps may need to be followed on the server platform.

10. All things are possible for the small environment, too

The more robust DR configurations tend to present themselves naturally to the large enterprise. However, the small IT shops are at a resource disadvantage when it comes to architecting a comprehensive DR plan. The ideal DR model would be applicable to big and small environments, and all of the objectives could be reached with the small organization. Technologies such as virtualization have really been a boon for the small environment to achieve their DR objectives, and that frequently is the cost justifier for the initial investments in storage and management software.

Don't overlook the human factor in your DR plan

By Mike Talon

Many organizations view disaster recovery planning as primarily a technology discussion and forget to take human nature into account. One of my clients went so far as to build a plan that relied on paying someone to grab disk drives prior to leaving the building in the event of a disaster. The company obviously left human nature out of its equation, and the entire DR plan was in serious jeopardy because of it.

When planning DR solutions, companies must remember that the technology will only supplement the efforts of humans in one way or another—not replace them. Whether the DR plan will keep systems online for client access (such as Web sites, ATMs, and intranets) or keep back-office solutions online, the main goal is to keep data available for people to use.

Human interaction impacts a DR plan on several different levels, and the IT staff is the most influential part of the DR plan. These are the people who must bring the operations back online during an emergency and keep them running. Never underestimate the role they play, even in automated DR solutions.

Not everything will work smoothly, due to misconfiguration or simple problems. When things go wrong, it will be up to your staff to fix the problems, as quickly as humanly possible.

When creating a DR plan, companies must be realistic, particularly about the people the plan involves. The people who set up the systems may not be available to perform failover operations. They may have left the organization, they may be unable to reach the systems in question, or they may be dead.

As horrible as the thought is, part of planning for disasters is planning for the worst-case scenario. While rare, large-scale disasters such as earthquakes can cause fatalities. You must plan for as many contingencies as you can—and hope that you haven't missed the one that actually happens when the disaster strikes.

Internal end users are another important factor in a DR plan. Bringing data systems back online will be a useless effort if no one can use them. Remember that you're planning for a multitude of possibilities, from power outages to building loss.

Most of these disasters will cause end-user desktops and access points to fail for one reason or another. While you can bring the data systems back online in another facility, you'll also need to find ways to get your end users up and running again.

VPN systems, alternate workspace, and other methodologies can help mitigate this issue, but you must plan for these options and set them up ahead of time. You also need to test them on a regular basis, and this means bringing end users into the testing process. Once again, the human element becomes a huge part of your DR planning.

Finally, don't forget that there's a good chance that the ultimate end users are not internal employees. There could easily be a large portion of data consumers who exist beyond the corporate firewall.

So not only must you set up alternate access for your internal concerns, but you must also be ready to reroute incoming and outgoing Internet connectivity as well. This may require DNS changes, additional connectivity links, and even additional security constructs such as signing certificates.

Nearly every Internet user expects occasional outages, but make sure that even if you can't get the original data center back online in a reasonable amount of time, you have some place for these clients to connect to within a short timeframe.

Never underestimate the impact of the human factor in planning for disaster recovery. Ignoring this element is a sure route to failure, and one that you can avoid by remembering that it still takes a human being to plug in a machine.

Sample Crisis Communications Policy

This policy has been established to ensure that in the event of a disaster or crisis, IT personnel will have a clear understanding of who should be contacted. Here are the topics you should address before a crisis occurs to ensure that communications can be quickly established in order to ensure business continuity.

Disaster recovery procedures for management

Each member of management will keep hard copy of the names, addresses, phone numbers, and non-work-related e-mail addresses of each employee in their units. In addition, management members will have a hard copy of the company's disaster recovery/business continuity plans on file in their homes in the event that the main building is inaccessible, unusable, or destroyed.

Contact with employees

Managers will serve as the "hubs" of their units, while designated employees will function as "nodes," calling other workers to discuss the crisis/disaster and the organization's immediate plans. Employees who cannot reach workers on their call list are advised to call the worker's emergency contact to relay information on the disaster.

Backup positions

If a manager or employee designated to contact other employees is unavailable or incapacitated, the designated backup employee will perform notification duties.

Notification of key executives

If key executives are unaware of the crisis/disaster, designated managers will contact them via e-mail or phone to relay news and follow-up planning. Managers will refer to the call list in their take-home documentation packs.

Recorded message/updates

For the latest information on the disaster and the organization's response, employees can call the hotline given in each worker's disaster recovery packet, which was distributed to you during your last annual review. Included will be information on the nature of the disaster, assembly sites, and directives on work resumption.

Vendors/insurance

Managers will refer to the accompanying list of all relevant vendors and manufacturers in the event that equipment, hardware, or software requires service or replacement. In accordance with company policy, please furnish the vendor with the following information: purpose of the equipment; when purchased/leased; cost; license; and version information. The company's CIO, or a backup if the CIO is unavailable, will contact insurance companies to assess next steps and to determine whether filing a claim is necessary.

Hot site/cold sites

If necessary, the organization's hot site at [location] will be activated and notification will be given via the recorded message or through communications with your manager. Staffing for the hot site will consist of managers only for the first 24 hours, with other employees joining the rest of the staff at the hot site the following day. If a cold site is identified and/or necessary, IT personnel will equip it with workstations for managers only until told otherwise.

Customer service

In-house customer service operations will resume at the hot site or cold site as soon as possible. As stated above, managers only are to report to the hot site within the first 24 hours or to the cold site after it is properly equipped. Customer service representatives will prioritize and address only the most critical calls as designated by their managers. For other common calls and requests, customer service representatives will send e-mails to customers that explain the current crisis and advise them on resolving common issues.

Documentation

Managers will have hard copies of all relevant documentation at an off-site location to ensure proper resumption of business activities as soon as possible. Managers will transport documentation to the hot site/cold site when directed to do so by unit vice presidents.

Signed: **Date:**

Disclaimer: This policy is not a substitute for legal advice. If you have legal questions related to this policy, see your lawyer.