

Getting Started With Disaster Recovery Planning

What you need in a disaster recovery (DR) plan

- ✓ **Authentication and validation tools:** All too often, a company's IT staff discovers that copies of crucial SSL certificates and important account passwords or physical access devices are missing when recovery is already underway. The solution: arrange for secure offsite storage of physical devices and for secure online storage of passwords and certificates with a third party. Practice their retrieval and use as part of your DR/BC drills, exercises and mockups.
- ✓ **Personnel contacts, info, and methods:** In a surprising number of cases, staff members discover that they can't reach the contacts identified in the disaster recovery or business continuity plan and plans too often fail to list a sufficient number of staff members to guarantee that a valid contact is available. Likewise, personnel notifications too often rely on somebody to manually initiate such contact by phone, email or other means.
- ✓ The solution: make sure a sufficient number of contacts are included to protect [recovery point objectives \(RPOs\)](#) and [recovery time objectives \(RTOs\)](#). Email and pager notification of key staff members should be arranged through a secure email account offsite. Some well-known providers include Yahoo, Gmail, or MSN, where you email passwords encrypted using a tool, like the [angel.net password applet](#), and make the account and password available to all responsible parties on the recovery plan staff list.
- ✓ **Geographical risks and factors:** Companies operate in earthquake zones, floodplains, fire hazard areas, and occasionally even in war zones without adequately planning for natural or manmade disasters. Check your situation carefully, and model the most likely disasters as accurately as you can when conducting practice drills. Make sure offsite or distant alternatives are identified in personnel information in case local staff is unavailable.
- ✓ **Recovery of individual computing:** During recovery, individuals and corporate IT assets such as servers and storage farms (SANs or NAS servers), need to get back to work. Make sure disaster practice addresses issues involved in providing desktop or notebook access to key staff members during recovery and to important staff members during the return to operational status.
- ✓ **Procure sufficient backup power and facilities:** Many companies discover that they can't draw on adequate power or facilities when they go into recovery mode. Practice sessions will quickly identify and help suggest remedies to such problems, but they can stymie recovery or continuity as surely as the lack of other important resources. Lack of sufficient power and facilities will show up during practice drills when and as drill teams try and fail to bring systems up because of power- or facilities-related issues or problems.
- ✓ **Identify priority order for resource recovery:** If servers need access to a storage server or farm before they can deliver access to key services or information, those resources must be ready before or as the servers come online. In general, most network resources will be unavailable until directory services are up, so they should be brought up first. Identify key dependencies and take them into account when documenting and describing recovery processes and procedures.
- ✓ **Provide adequate documentation and instructions for recovery:** Beyond addressing essential dependency issues covered in the preceding item, many companies discover during recovery that some aspects of their processes and procedures are missing, insufficiently detailed or lacking important information. Creating "The Book" and going by that book during practice drills helps highlight oversights and omissions and see them addressed before genuine disaster or business interruption strikes.

- ✓ **Exercise DR/BC plans regularly and rigorously:** At least yearly, companies must work their way through DR/BC plans completely and thoroughly and dispassionately record all issues, oversights, omissions and errors for quick follow-up remediation. There is no substitute for practice and thorough testing in this arena.
- ✓ **Keep your DR/BC plans current and corrected:** It's essential to put processes in place that require staff to report regularly on plan status, and enact change management to keep plans in synch with organizational and technical realities on the ground. It's also important to perform regular audits to check how well plans and reality match.
- ✓ **Regular attention and involvement:** Executives, IT staff, key department heads, and other staffers must remain aware and tuned into disaster recovery and business continuity needs, priorities, and information. Some companies go so far as to make recovery drill participation mandatory, and a checkbox item for annual or periodic performance and salary reviews (tying participation to raises seems to be a powerful motivator). Ultimately, that's the only way to make sure that DR/BC plans completely address the return to business as usual even when disaster strikes.

Ten things that must be included in an IT disaster recovery (DR) plans

1. Disaster recovery plans must have an accurate communication or call list.

Communicating with other employees is essential during a disaster. Your call list must always be kept current. The list should have designated backups for each key individual and multiple contact information for them as well. If you are using a call tree, make sure that you have a loop back so that the last person on the list will confirm that the call was made. Also, someone should be designated as the communication list manager to monitor responses and contact backup staff as necessary.

2. Work from a detailed script during a disaster.

When you are in recovery mode, many things occur at the same time, and confusion is a given. In order to make the disaster recovery process easier, have a detailed script or step-by-step instructions in your [DR/BC plan](#). The script should be formally reviewed by several different members of the DR team. And since there is no guarantee that the script will be followed by the same person who wrote it, it's best to use a simple bulleted list with easy-to-follow steps. When in a real recovery scenario, there will be intense pressure and many things going on at the same time. Also, a disaster can occur at any time, so if the plan is executed late at night, confusion is likely to be high. Whatever can be done in the plan to make the steps easier to follow will go a long way. If at all possible, try to anticipate errors and include remediation steps. An example bulleted point can be as follows: "Connect network cable to PC. If network not found, first check if PC Ethernet connection shows signal." Straightforward and simple instructions go a long way when you are under extreme stress and fatigue. Avoid using terms that may not be understood when extreme fatigue hits. If you must use technical terms that may not be understood, add a glossary of terms.

3. Test and retest the detailed disaster recovery plan.

It is possible to test separate portions of the DR plan on their own, but make sure the whole plan is tested at least once a year or if a major change takes place. If you exercise or test the DR plan at least once a quarter, then the staff will become more familiar with the plan. And to make it more effective, try to exercise the plan with different staff members if you can. When testing the DR plan, don't assume that everything will go according to plan -- this is why it's important to test. Always anticipate unusual conditions. For example, you must come up with solutions for unexpected events, i.e. what would the team do if a drive or a technical component fails?

4. Each member of the team should be familiar with his or her defined role.

Additionally, the backup members must be familiar with their roles. If a team member whose primary role is applications has a backup role as a telecommunications resource, make sure they know what that role entails.

5. Have a list of 24-hour supply delivery resources and restaurants at the recovery site.

This next item may sound odd as a "must have," but it is of utmost importance sometimes. You will likely spend many hours at a recovery site and will need to replenish supplies. You do not want to start searching for places when every minute and resource counts. You may very well need to be at the recovery site for longer than 24 hours at a time. Also, be sure you know where the nearest hardware and office-supply stores are at your recovery site.

6. Include an application list in the DR plan.

An application list is any software package or system that will be part of the recovery, and it should always appear in a master list. Each entry in the list should have the application name as the technical staff identifies it, the name the business side recognizes, and any technical details such as server name, etc. Along with the technical items, include the application owner, their full contact information, and backup contacts.

7. Include a current network diagram of the entire network and recovery site in the DR plan.

Each node on the switch and panels should have some means of identification. In a recovery, you do not want to start following cables and wires through switches, etc.

8. The DR plan should contain an easy-to-follow map and directions of how to reach the recovery site.

Do not assume everyone knows how to get to the recovery site. Secondary directions should be provided too in case the main route is congested or impassable. Also, include available parking facilities.

9. Include additional documentation such as a list of vendor contacts and insurance documentation such as policy numbers.

These items as well as a list of all the hardware and software licenses you may have are helpful to have in a disaster recovery plan.

10. The disaster recovery plan must be current.

The most critical issue regarding a disaster recovery plan is that it is current and that a backup copy exists at the recovery site. You do not want to go through a recovery process with an outdated plan. In order to avoid this, update the plan at least once a year, or whenever modifications are made that require a change in the disaster recovery plan. These changes can be in hardware, software upgrades virtualized servers, or any change that would modify the current disaster recovery environment.

IntegrIT Network Solutions is here to help you with your [business continuity planning](#) and [disaster recovery](#) needs. Our business continuity planning experts incorporate industry-leading best practices to create responses to almost any type of disaster or unplanned events. Together we'll create a business continuance organizational plan that clearly outlines the actions and responsibilities to help recover and restore critical operations. And with the expertise of the IntegrIT team, this plan will continue to evolve, producing new responses as potential threats develop. Each day that companies put off their continuity planning increases the risk of total loss. Don't wait to start the conversation.