How to Complete the IT Disaster Recovery Plan

This instruction guide gives you step-by-step instructions for completing your organization's IT Disaster Recovery (DR) Plan. It really, really, really helps to have performed a BIA prior to writing this plan. So you haven't done that yet, we highly recommend that you consider it, as it'll provide a good roadmap for the IT Disaster Recovery plan.

The IT department really should take the lead in developing this plan. Unless the BC Coordinator is within the IT department, his or her role will be one of advising and explaining connections to other parts of the program.

As with the other plan instructions, we'll focus on the areas that require more than a simple review…the areas that require explanation or guidance.

Steps to follow to complete the Crisis Management Plan using the template provided:

Section 1. This is actually an important element of the plan, more than you might think. This indicates what you are actually planning to recover from. This is sort of a "reasonable worst case scenario." The loss of a data center or internet service provider is a different kettle of fish than a simple hardware failure. Simple hardware failure is sort of a cop-out when it comes to DR planning. But you have to know your assumption going into the plan, or else people's interpretations will be all over the board. Good practice is to assume your primary data processing facility (internal or outsourced data center) will be inoperable for 2 weeks.

Section 2. Building on Section 1, even though you created an assumption to guide planning, you should be able to respond to other IT events as well. Take the time to list those here. We've given you some examples.

IT departments are organized in all shapes and sizes, so our example structure might not apply to your organization. Have the IT department ask itself, "If our planning assumption (i.e. data center failure) occurs, which groups will need to support recovery, and why?" By asking those questions, IT should be able to identify the key groups and establish their responsibilities.

Section 3. Review for necessary modifications to meet your company's needs.

Section 4. We've found that including an overview of recovery strategies is a good "quick reference" covering the types of issues that IT may have to deal with. We're only talking a sentence or 2 for each area. The overview is a good way to get out of the weeds and see the big picture. As necessary, recovery procedures related to any of these areas can be included in the next section.

Section 5. In this section, IT will include appropriate recovery procedures to recover from the "assumed disruption." Consider this section the "nuts and bolts" of the plan. For each recovery activity, include:

a. What tasks need to be performed? By whom?
b. Who needs to know about it, or who needs to assist with the task?
c. How will required resources be obtained?
d. How will IT verify that recovery is complete, and who will be notified of that?

Try to list the activities in chronological order. That'll provide more organization if you actually have to go through all of the procedures you've identified.

A note on the level of detail: DR plans vary in detail from company to company. It is good practice to assume that people are competent in their jobs, but need guidance on what to do during a disaster. IT employees probably only need to know how to perform the steps that are done infrequently, maybe they only apply during a disaster and employees aren't familiar with the procedures. By all means, list those procedures in detail. If there are tasks that are performed on a daily basis, you probably don't need to spell those out in the DR plan. Your IT department should know which tasks are routine, and which are not.

Section 6 gives a prioritized view of the applications that are critical to the business. The prioritization provides guidance to IT if multiple applications require recovery. The table also shows the recovery time objective and amount of data loss (referred to by BC geeks as the "RPO", the Recovery Point Objective). Ignore that if you want; what you need to know is the time between backups. It is not uncommon for business applications to be backed up nightly. Some might be backed up or replicated every 15 minutes, or real-time. It all depends on what your IT department has configured. A good deal of this information was gathered during the Business Impact Analysis, so make sure to refer to it.

Section 7. Here's is more plan content that ranges widely from company to company. The purpose of this section is to allow to quickly identify and purchase new equipment if any is damaged. This doesn't have to be a complete IT hardware inventory; it can focus on those items that are the most vital and time sensitive. Again, your IT department should know how much detail is necessary.

Section 8. Like every plan, you'll want to be able to communicate with others quickly, that true for internal and external parties. List those people or groups in this section. Internal contacts may be those departments that are most impacted by the outage. External contact are most likely those who would be involved in helping you recover from a disruption (e.g., 3rd party alternate data center, etc.)

Appendix A – Network Diagram. Include a network diagram to include backup and failover configurations if that'll help you assess the situation and make better decisions. A bunch of technical diagrams in the DR plan may not help, so be selective in what you use.

