



Creating a Disaster Recovery Plan

Presented by

J Costa Consulting

<http://www.costatech.net>

What would you do if a storm flooded your server location? Or how would you respond if a power outage blacked out your systems? How would you recover your data and keep the business running after an unforeseen disaster? When disasters strike unprepared companies the consequences range from prolonged system downtime and the resulting revenue loss to the companies going out of business completely, yet many businesses are not prepared to deal with such scenarios.

The key to surviving such an event is a business continuity strategy, a set of policies and procedures for reacting to and recovering from an IT-disabling disaster, and the main component of a business continuity strategy is a disaster recovery plan (DRP).

Step 1: Risk Analysis

The first step in drafting a disaster recovery plan is conducting a thorough risk analysis of your computer systems. List all the possible risks that threaten system uptime and evaluate how imminent they are in your particular business systems. Anything that can cause a system outage is a threat, from relatively common manmade threats like virus attacks and accidental data deletions to more rare natural threats like floods and fires. Determine which of your threats are the most likely to occur and prioritize them using a simple system: rank each threat in two important categories, probability and impact. In each category, rate the risks as low, medium, or high.

For example, a small company (less than 50 employees) located in Florida could rate a hurricane threat as medium probability and high impact, while the threat of utility failure due to a power outage could rate high probability and high impact. So in this company's risk analysis, a power outage would be a higher risk than a hurricane and would therefore be a higher priority in the disaster recovery plan.

Step 2: Establish the Budget

Once you've figured out your risks, ask 'what can we do to suppress them, and how much will it cost?' Can I detect a threat before it hits? How do I reduce the potential of it occurring? How do I minimize its impact to the business? For example, our small Florida company could employ an emergency power supply to mitigate its power outage threat and have all its data backed up daily on a secured remote site in case of an hurricane. The more preventative measures you establish upfront the better., "Dollars spent in prevention are worth more than dollars spent in recovery."

The results of Step 1 should be a comprehensive list of possible threats, each with its corresponding solution and cost. It is imperative that an audit of all of these threats to the business completed and presented to the business operations units, so they can make an informed decision regarding the size of the disaster recovery budget (i.e., which risks the company can afford to tolerate and which it must pay to mitigate). Systems managers "falls down" in their failure to communicate the real risks for system downtime to the business operations units of the companies. "It's okay for operations to say no; it's not okay for the business operator to not know about the risks."

A good place to begin is by understanding the cost of downtime by the responsible person for the business. How long can your business afford to be without its computer systems should one of your threats occur?

Ultimately, the business operations unit decides which threats the business can tolerate. When developing a DRP, consultants are "shooting in the dark without those business indications." Both the consultant and the business unit must agree on which data and applications are most critical to the business and need to be recovered most quickly in a disaster. The management of our small company, for example, may decide they can supply the budget only for the emergency generators and the company will have to assume the risk of a hurricane.

Disaster recovery budgets vary from company to company but they typically run between 5 and 10 percent of the overall IT budget. Companies for which system availability is crucial usually are on the higher end of the scale, while companies that can function without it are on the lower end. However, these percentages may be too small. For a medium business 15 percent is a best practice rule of thumb.

Step 3: Develop the Plan

The feedback from the business units will begin to shape your DRP procedures. If, for example, they determine that the company must be up within 48 hours of an incident to stay viable, then you can calculate the amount of time it would take to execute the recovery plan and have the business back up in that timeframe. We suggest that you have the recovery systems tested, configured, and retested 24 hours prior to launching them. The set up takes anywhere from 40 hours to days to complete.

The recovery procedure should be written in a detailed plan or "script." Establish a Recovery Team from among the staff and assign specific recovery duties to each member. The manner in which your team conducts its recovery probably will be no different than its regular production procedures: the chain of command likely won't change and neither will the aspects of the network for which each member is responsible.

Define how to deal with the loss of various aspects of the network (databases, servers, bridges/routers, communications links, etc.) and specify who arranges for repairs or reconstruction and how the data recovery process occurs. The script will also outline priorities for the recovery: What needs to be recovered first? What is the communication procedure for the initial respondents? To complement the script, create a checklist or test procedure to verify that everything is back to normal once repairs and data recovery have taken place.

Step 4: Test, Test, Test

Once your DRP is set, test it frequently. Eventually you'll need to perform a component-level restoration of your largest databases and data to get a realistic assessment of your recovery procedure, but a periodic walk-through of the procedure with the Recovery Team will assure that everyone knows their



roles. Test the systems you're going to use in recovery regularly to validate that all the pieces work. Always record your test results and update the DRP to address any shortcomings.

As your business environment changes, so should your DRP. Reexamine the plan every year on a high level: Do you still need every part of the plan? Do you need to add to it? Will the budget need to be adjusted to accommodate changes to the plan? As applications, hardware, and software are added to your network, they must be brought into the plan. New employees must be trained on recovery procedures. New threats to business seem to pop up every week and a sound DRP takes all of them into account.