

Seven steps to disaster-recovery planning

By Bruce Beaman and Becky Albin, Network World , 06/25/2008

Copyright 2008 by Network World. All rights reserved.

This vendor-written tech primer has been edited by Network World to eliminate product promotion, but readers should note it will likely favor the submitter's approach.

Unpredictability is a fact of life. Whether terrorist attacks, cataclysmic weather or simply a backhoe severing a power cable, enterprises never know when their operations may be threatened.

But mitigating the consequences of disasters need not be a matter of worry and guesswork. Here are seven steps to effective business-continuity/disaster-recovery (BCDR) planning that will provide some practical guidance.

Step 1 – Admit the possibility of disaster

Just as the first step to personal recovery is admitting one has a problem, so the first step in BCDR planning is to admit the organization faces tangible threats that could jeopardize its prosperity – or its survival. Until this first step is taken at a senior leadership level, go no further.

Step 2 – List and categorize likely threats to the organization

The nature of the business and its physical and social environment will influence the types of threats an organization might face. Once the threats are listed, they should be categorized according to their likely impact on various systems. The cost of the response should be balanced against the tolerance for system downtime -- the less downtime that can be tolerated, the more it will cost to create an appropriate response. Some systems must be functioning again within minutes or seconds, while others can be down a few hours, and still others can be down for a few days without serious consequences.

Step 3 – Outline the organization's BCDR technology infrastructure

The key technology elements of a BCDR infrastructure consist of a main [data center](#), a remote site that duplicates the resources in that primary location, and high-bandwidth network connections. The best BCDR strategies follow a “redundant everything” philosophy throughout the data center. Multiple mainframes and servers should run in the production and backup data facilities. Then if a component in the production system encounters problems, it immediately fails over to the local backup as a first line of defense.

Power supplies are one of the most critical components in a BCDR strategy. Power outages rank among the leaders in most common and preventable disruptions, according to industry analyses.

And no matter how fat the network pipe may be, it's of little use if a careless construction crew accidentally severs a fiber. Network connections must not only be redundant, they also need to follow different paths within a wider WAN topology to keep a single threat from bringing businesses to a standstill.

Step 4 – Inventory the organization's IT assets

Once organizations have sketched out the topology of their BCDR infrastructure, the next step is to develop an accurate inventory of IT assets. This enables the organization to understand the resources and business processes that need to be protected.

A range of enterprise management tools are available to help organizations develop and maintain accurate inventories of IT resources. Vendors of these tools offer modules that use software agents to scour the IT infrastructure, storing details about hardware and software assets and their configuration parameters in configuration management databases (CMDB).

Step 5 – Set service-level expectations and define contingency policies

CMDBs store not only the details about the organization's software and hardware assets but also information about service-level agreements that define the uptime and recovery parameters for those assets. Recalling Step 2, it is important that senior management buy into service-level expectations, because these will determine (among other things) whether a particular asset must be up and running within 5 minutes or 5 hours of an outage. This determination directly influences BCDR expenditures that senior management will later be asked to support.

Based on a clear knowledge of assets, configurations and service-level agreements, an organization can define contingency policies. These policies must have executive-level support, and will therefore need to link IT asset performance directly to business requirements. In order to form this important linkage, the organization will need to perform a business impact analysis to flesh out details about system requirements, processes and systems inter-relationships. Executives must understand the consequences of system disruptions in order to support (and fund) contingency policies.

Step 6 – Develop a BCDR contingency plan

Flowing directly out of contingency policies, the contingency plan details the roles and responsibilities of departments and individuals in keeping technology systems available, as well as the procedures for restoring IT systems during an emergency. Key elements of contingency planning also include resource requirements, training needs, the frequency of training exercises and testing, maintenance schedules, and data-backup schedules.

The phases of a contingency plan include the initial notification/activation when the emergency strikes, restoration/recovery once emergency teams have been mobilized, and finally a return to normal operation (or a decision to remain on backup resources in the case that primary resources must be replaced or rebuilt over a significant period of time).

Step 7 – Test the BCDR contingency plan

Disaster-recovery experts say one of the most important yet frequently overlooked aspects of disaster-recovery planning comes after the formal policies and procedures are delineated. Plans

must be tested initially for their completeness and effectiveness, and then retested on an ongoing basis to make sure that any subsequent changes to the IT infrastructure and business processes haven't created a need for policy modifications.

In addition, organizations should create test beds that accurately reflect day-to-day business conditions, so that drills simulate real-world conditions.

The world may be too complex for organizations to protect against every disaster contingency, but with the right technologies, clear service-level expectations, practical recovery policies, thorough contingency plans and rigorous testing methodologies, organizations can minimize the business consequences when the unexpected happens.

Beaman is senior director of Adabas Product Marketing at Software AG, and Albin is chief IT architect of Software AG. Contact them at bruce.beaman@softwareagusa.com and becky.albin@softwareagusa.com