Ken's Korner

DISASTER RECOVERY PLANNING

With data center downtime costing on average $7,900 per minute, a minor power loss or system failure outage can be costly, but a major outage could be devastating, costing a business hundreds of thousands if not millions of dollars. Employing a well thought out disaster recovery plan offers two primary benefits, first the process of implementing disaster recovery policies and procedures will facilitate a quicker recovery from power outages and system failures and the process of evaluating processes and systems will limit the occurrence of avoidable outages and downtime.

> *The average cost of an unplanned data center outage is $7,900 per minute, a 41% increase since 2010. The average outage lasted 86 minutes resulting in an average cost per incident of $690,000.*
> *Ponemon Institute: 2013 Study on Data Center Outages*

Know your risks

Each individual data center's geographic location represents inherent risks. Tornado's, hurricanes, floods, fires. When evaluating your individual data center, first consider its environment as part of its disaster recovery plan.

Knowing your risks carry over to the data centers infrastructure and supporting vendors. If you are operating with older equipment you may be at greater risk for system failures and outages. If your supporting vendors aren't as dependable as you'd like or have to travel a greater distance to service the equipment, you may need to take extra precautions when planning for outages.

Addressing the causes not just the symptoms

Have a plan to address in a step-by-step process what you want your people to do if there is an outage, any outage. Having written guidelines, processes and procedures decreases the likelihood that you'll miss something when troubleshooting outages. Even if the problem appears to be obvious and easy to fix, after resolving the outage, you'll want to go back through your recovery plan to verify that no other systems have been affected by the outage. There may be underlying causes waiting to trigger another outage, inevitably at a critical time for the data center.

Recognize your systems weak spots

UPS battery backups and diesel generators are the two most common causes of unplanned outages. If you know these and other areas represent weak spots in your infrastructure, increase your maintenance schedule, change parts more frequently, or consider getting your staff concentrated training on each piece of equipment.

Being prepared for outages

The most important part of a disaster recovery plan is the part that addresses how to prevent outages and system failures from occurring. While over 90% of all data centers report having an unplanned outage within the past 24 months, the steps you take to prevent the outage in the first place will help as much to determine the duration of the outages as it does the frequency.

> *There are experts that can help you design and test a Disaster Recovery Plan.*
> *This is a great place to start the process.*

PDU :: Cables™
connect with us™

5401 Smetana Drive
Minnetonka, MN 55343
(866) 631-4238 Toll-Free
(800) 336-2801 Fax
www.pducables.com

Ken Koty; former data center facilities manager with over 30 years of hands-on experience shares management practices that made him a 12 year award recipient for continuous uptime from the Uptime Institute. PDU Cables does not guarantee the results of outcomes by using information contained in this document..

DISASTER RECOVERY PLANNING (CON'T)

Documentation
√ As part of your disaster recovery plan (DRP), assign DRP books to each member of your staff as well as keep DRP books at various stations throughout the data center.
√ Keep a master DRP book on site and off site.
√ As information changes, distribute updates for each book.
√ Each book should contain building plans, floor plans, system maps, network diagrams and equipment configurations. The book should also document location of entrances and exits, raised floor area, and external to the building fuel storage tanks, power substations, proximity to roads and highways, rail lines and airports.
√ The DRP book should have a listing of key personnel, main phone numbers, cell numbers and other contact information.

Managing personnel
√ Assign staff specific duties to perform in case of a disaster.
√ Document staff assignments for all to know.
√ Provide written documentation for each DRP task.
√ Regularly review DRP policies and procedures.
√ Cross train all tasks to account for vacations and sick-time.
√ Confirm on-site support from outside vendors.

Creating a disaster recovery plan (DRP)
√ Identify scenarios for each possible data center outage or incident. Scenarios should include both simple short duration disruptions; power outage, server failure and major long duration disruptions; flooding, building damage and fire.
√ Walk through each scenario and identify action items and assign duties and responsibility to appropriate staff members.
√ Steps should include assessing the extent and nature of the disruption, identify causes, run diagnostics, assess damage to related systems, and remember to provide regular updates to senior management on the status of the recovery.

Testing your disaster recovery plan (DRP)
√ When testing a DRP, make sure you have complete, tested and proven procedures. If you find that there are additional steps necessary to execute the DRP that are not documented, use this time to record and refine the new steps.
√ Identify the personnel to complete each individual process in the DRP, and make sure they have the tools, training and capabilities to execute their job.
√ Assign backups for each of your staff, in case someone is on vacation or physically unavailable to participate.

√ Executing a DRP is a team effort and like many team activities, assigning too many responsibilities to too few people can potentially slow the recovery process.
√ Testing should identify missing or incomplete steps in the DRP, make changes and modify the plan as needed.
√ Testing will give you a more accurate time frame for how long it will take to implement your DRP.
√ When testing a DRP, make sure backup data centers are able to handle your primary data center's load/customers.
√ When performing DRP tests, make sure to vary the time of day and day of week of your tests to create a greater sense of surprise and a more realistic test environment.
√ Online disaster recovery plans are convenient as long as they are accessible, hard copies kept on site may be necessary.

Additional considerations
√ If backup site has limited capacity, identify critical tasks or functions to be transferred to the backup site as part of a DRP.
√ If using a backup data center, practice shifting management of data center to the backup location.
√ The duration of the disruption or condition of the site after the disruption will often dictate how long the outage lasts.
√ How fast can you get additional diesel fuel if power takes days or even weeks to be restored? It pays to do business with multiple fuel provider in the event of an emergency. In some cases you can make an agreement with the providers that they will deliver a fuel request within a named time.
√ If you are using open water cooled towers where will you get additional water if the water supply is interrupted? At our data centers we invested in having our own water wells installed with the ability to keep our cooling systems running.
√ Our data centers also had several data paths to enable us to get our information to our customers.
√ If your site is destroyed from a major issue like fire, flood, bad weather etc., have you made sure your back-up site is able to deal with your online load.
√ Is their site staffed with the properly trained personnel to handle your business in the event you are not able to get additional people to their site, especially support from equipment vendors or normal maintenance crews?
√ What type of disaster recovery plan do they have and are their people trained and tested on it.

PDU :: Cables™
connect with us™

Remember, when it comes to maintaining uptime and recovering after an outage, only thorough planning, regular testing and preventative maintenance will ensure success.