vmware®

The Top Ten Most Forgotten Things When Building a Disaster Recovery Plan

Every IT manager knows the importance of having an effective disaster recovery (DR) plan. Organizations without an adequate plan may find themselves out of business quickly after experiencing a major disaster. This statistic is amplified for small and midsized businesses: many of these businesses today are relying on archaic backup and restore plans that will certainly not enable them to survive many of the disasters seen lately or the frequency of everyday mishaps that impact IT.

Organizations that want to ensure survival following a disaster may already understand the basics of creating a good plan; however, there are many obstacles and pitfalls that they can easily avoid. Based on working with thousands of customers, we've come up with the following top ten checklist. Take a look to make sure you haven't missed a crucial step that could make the difference between staying open or going under!

Hopefully your business will never have to experience a major disaster. But having an effective disaster recovery plan with sufficient documentation, adequate testing, and well trained staff will increase your chances of survival when faced with a minor or major catastrophe.

Interested in learning more about the positive impact VMware virtualization can have on your businesses' survival?

Learn more by visiting www.vmware.com/smb.

1. **Failing to identify everything that could potentially jeopardize the infrastructure and data that run your business.** In addition to the obvious threats – viruses, Trojans, worms, etc. – you need to identify any forces that are unique to your geography. Do you live on an earthquake fault or in a flood zone? Does your region experience frequent power interruptions from storms or rolling blackouts? Make sure all of these possibilities are considered when creating your plan or choosing a location for a new DR facility.

2. **Creating a plan that depends on too few qualified personnel.** It is not uncommon for businesses to create a DR plan that depends on just one IT person with a pager. What if that person is unavailable for some reason? You need to identify and cross-train a pool of employees that are capable of responding in an emergency. It also helps if this pool of resources is geographically dispersed in case of a large environmentaldisaster that affects all local employees.

3. **Relying on manual processes to notify staff during a disaster.** If the power goes out in your facility and no one is there to report it, will your DR staff be informed? You need to create an automated system that will notify your IT staff of any disaster or disruption to service. You can also establish an arrangement with a third-party service provider to monitor your facility and notify a pre-defined set of individuals that are trained to execute your DR plan.

4. **Failing to procure adequate backup power.** If your facility is affected by a wide-spread environmental disruption, you many find yourself without power for an extended period of time. Be sure to purchase the longest-life, most uninterruptible power supply available. Then obtain additional battery back-up for continued power.

5. **Forgetting to prioritize what resources need to be restored first.** Which of your IT applications need to be accessed first? Are there some that can wait a day or two without affecting your business? You need to be selective about the order in which applications and services are brought back online first after a disaster. For example, you might choose to reactivate your company's email application before you restore departmental file servers. There may be politics involved in this decision, so make sure you get buy-in beforehand, to avoid the "me firsts!"

6. **Failing to create adequate documentation of your DR plan.** After creating a plan, be sure that you create detailed step-by-step instructions on how to execute the recovery plan. Ensure that every process is well documented. Describe the location of all system resources needed to accomplish the recovery. Be sure to store the documentation at multiple locations and verify that all key personnel have easy access to the manuals.

7. **Relying on back ups.** It doesn't matter how good your DR plan is if your data is out of date, is in a location also affected by the disaster, or has become corrupted. Perform backups at rigidly enforced, regular intervals to protect information integrity. Or, use a technology like VMware virtualization to implement a remote site with replicated virtual machines to speed recovery.

8. **Forgetting to test your disaster recovery plan.** You need to make sure your recovery plan actually works in an emergency! While this seems obvious, many enterprises neglect to adequately test their plans. You should regularly conduct data fire-drills to test every possible scenario, from basic power failures to catastrophic events that could result in multiple months of devastation. Again, technology like VMware virtualization, and the ability to to provision any server with the virtual machines needed, in minutes, make testing your DR plan fast and effective.

9. **Making passwords too hard to find.** Though password protection is a key goal for data security, you need to store your system passwords in at least two geographically separate, secure locations. Make sure that more than one IT staff person has access to all passwords and codes. And be sure to change these passwords promptly if key personnel leave the company.

10. **Failing to keep your recovery plan up to date.** You should never stop updating your DR plan. Once you've created your plan, revisit it at least on a quarterly basis. Determine a list of trigger points that should invoke changes to the plan, like personnel, equipment, location or application changes, to name a few. This will not only keep your IT staff's skills fresh, it will also provide the opportunity to improve procedures as you uncover vulnerabilities in your plan or ways to streamline your procedures.

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com