DR Planning for SMBs

Improving DR plans is always top of mind for storage professionals at small and medium sized organizations. This guide provides storage pros with the necessary information to improve the effectiveness of their overall DR plan. You’ll learn what to be aware of when putting a DR plan in place, as well as what every DR plan should have.
Table of Contents

Small business disaster recovery planning strategies

What you need in a disaster recovery (DR) plan

Resources from CA ARCserve
Small Business Disaster Recovery Planning Strategies

Jeff Byrne

Disaster recovery (DR) is increasingly becoming a critical mandate for small- and medium-sized businesses (SMBs). The cost of downtime -- and lost data can be a major caveat for any size organization. And it doesn't take a cataclysmic event to cause major disruption to a small business: the untimely loss of a critical file, server or application, even just for a few hours, can be extremely costly.

In addition to the costs involved, a number of industry-specific regulations now require that even a moderately sized organization be able to demonstrate that its key business and IT assets are protected and/or fully recoverable in the event of a disaster. Less-than-full compliance with such regulations can result in the reprimand or firing of the managers responsible, along with severe penalties to the company itself.

And yet, despite the costs and risks of operating without a disaster recovery strategy, many small businesses are not prepared to cope with the stresses of a disruptive outage, let alone a full-fledged disaster. Based on a Taneja Group survey of hundreds of IT managers conducted in mid-2009, more than one-half of SMBs based in North America do not have a disaster recovery plan in place. Unfortunately, roughly one-quarter of the SMBs responding to the survey have suffered a significant outage in their IT infrastructures during the past three years.

Disaster Recovery Tools of the Trade: Small Business Disaster Recovery Tips

Before we look at what goes into a disaster recovery plan for a small business, let's take a quick look at some disaster recovery tools and technologies introduced during the past five to 10 years that can help take some of the cost and complexity out of a DR infrastructure. These resources are based largely on software rather than hardware, and therefore enable greater flexibility and a lower upfront investment. In fact, one could argue that for the first
time, these technologies actually make enterprise-grade DR affordable for small to medium sized businesses.

The first of these technologies is server and storage virtualization. Virtualization significantly reduces the dependence of applications and data on hardware platforms, while greatly increasing their mobility. When combined with wide-area network (WAN) acceleration, these technologies open up new disaster recovery opportunities for small businesses. One popular DR approach in VMware environments is to take a snapshot of a running virtual server -- including its operating system, configuration settings, data and applications. After that, replicate that snapshot image to a remote site. Since incremental snapshots are now both space-efficient and non-disruptive, they can be taken as frequently as required to satisfy recovery time objective (RTO) and recovery point objective (RPO) metrics. Small and medium businesses that cannot afford the luxury of a single, designated disaster recovery site can set up data replication paths between different branch or remote sites, to at least cover the risk of a single-site failure.

Going one step beyond snapshot replication, virtualization and data protection, vendors are now offering automated failover capabilities for virtual machines (VMs), which will be supplemented in the near future with automated failback functionality. Products such as IBM Tivoli Storage Manager (TSM), Symantec Veritas Cluster Services (VCS) and VMware Site Recovery Manager (SRM) offer automated VM failover at varying levels today. Though only a handful of SMBs are using such automated tools today, we believe they will become increasingly more attractive to SMBs from both a cost and manageability standpoint.

Learn about common pitfalls in disaster recovery procedures in the next part of our guide on small business disaster recovery planning.

**About this author:** Jeff Byrne is a senior analyst and consultant at the Taneja Group, an analyst firm focused on storage and storage-centric server technologies with a concentration in the developing area of virtualization. He can be reached at jeff.byrne@tanejagroup.com.
What you Need in a Disaster Recovery (DR) Plan

Ed Tittel

Recent reports indicate that as many as half of all small- to medium-sized businesses (SMBs) lack a business continuity (BC) plan or a disaster recovery (DR) plan. Those who do formulate plans often discover they lack certain information or coverage when the time comes to put them to work. Besides underscoring the need for regular mock exercises in implementing disaster recovery and business continuity plans, this phenomenon also underscores the costs of human frailty and oversight in putting such plans together. Here’s my list of items that you need in a disaster recovery plan. A good disaster recovery plan is key to a successful disaster recovery program. These are some things that companies often discover missing in their disaster recovery plans:

1. **Authentication and validation tools:** All too often, the IT staff discovers that copies of crucial SSL certificates and important account passwords or physical access devices are missing when recovery is already underway.
   The solution: arrange for secure offsite storage of physical devices and for secure online storage of passwords and certificates with a third party. Practice their retrieval and use as part of your DR/BC drills, exercises and mockups.

2. **Personnel contacts, info and methods:** In a surprising number of cases, staff members discover that they can’t reach the contacts identified in the disaster recovery or business continuity plan and plans too often fail to list a sufficient number of staff members to guarantee that a valid contact is available. Likewise, personnel notifications too often rely on somebody to manually initiate such contact by phone, email or other means.
   The solution: make sure a sufficient number of contacts is included to protect recovery point objectives (RPOs) and recovery time objectives (RTOs). Email and pager notification of key staff members should be arranged through a secure email account offsite. Some well-known providers include Yahoo, Gmail or MSN, where you email passwords encrypted using a tool like this password applet [http://angel.net/~nic/passwd.sha1.1a.html], and make the account and password available to all responsible parties on the recovery plan staff list.
3. **Geographical risks and factors:** Companies operate in earthquake zones, floodplains, fire hazard areas and occasionally even in war zones without adequately planning for natural or manmade disasters. Check your situation carefully, and model the most likely disasters as accurately as you can when conducting practice drills. Make sure offsite or distant alternatives are identified in personnel information in case local staff is unavailable.

4. **Recovery of individual computing:** During recovery, individuals and corporate IT assets such as servers and storage farms (SANs or NAS servers), need to get back to work. Make sure disaster practice addresses issues involved in providing desktop or notebook access to key staff members during recovery, and to important staff members during the return to operational status.

5. **Procure sufficient backup power and facilities:** Many companies discover that they can't draw on adequate power or facilities when they go into recovery mode. Practice sessions will quickly identify and help suggest remedies to such problems, but they can stymie recovery or continuity as surely as the lack of other important resources. Lack of sufficient power and facilities will show up during practice drills when and as drill teams try and fail to bring systems up because of power- or facilities-related issues or problems.

6. **Identify priority order for resource recovery:** If servers need access to a storage server or farm before they can deliver access to key services or information, those resources must be ready before or as the servers come online. In general, most network resources will be unavailable until directory services are up, so they should be brought up first. Identify key dependencies and take them into account when documenting and describing recovery processes and procedures.

7. **Provide adequate documentation and instructions for recovery:** Beyond addressing essential dependency issues covered in the preceding item, many companies discover during recovery that some aspects of their processes and procedures are missing, insufficiently detailed or lacking important information. Creating "The Book" and going by that book during practice drills helps highlight oversights and omissions and see them addressed before genuine disaster or business interruption strikes.
8. **Exercise disaster recovery and business continuity plans regularly and rigorously:** At least yearly, companies must work their way through DR/BC plans completely and thoroughly and dispassionately record all issues, oversights, omissions and errors for quick follow-up remediation. There is no substitute for practice and thorough testing in this arena.

9. **Keep your DR/BC plans current and corrected:** It’s essential to put processes in place that require staff to report regularly on plan status, and enact change management to keep plans in synch with organizational and technical realities on the ground. It’s also important to perform regular audits to check how well plans and reality match.

10. **Regular attention and involvement:** Executives, IT staff, key department heads and other staffers must remain aware and tuned into disaster recovery and business continuity needs, priorities and information. Some companies go so far as to make recovery drill participation mandatory, and a checkbox item for annual or periodic performance and salary reviews (tying participation to raises seems to be a powerful motivator). Ultimately, that’s the only way to make sure that DR/BC plans completely address the return to business as usual even when disaster strikes.
Resources from CA ARCserve

Disaster Recovery for SMBs

Essential Guide to Data Backup for SMBs

E-Guide: SMB Essentials-- Backup, Dedupe, and DR best Practices

About CA ARCserve

The Recovery Management and Data Modeling Business Unit of CA Technologies (NASDAQ: CA) delivers the acclaimed CA ARCserve and CA ERwin products. Providing much more than backup, the CA ARCserve Family of Products gives customers control over their changing business by delivering total protection, recovery and availability for systems, applications and data – across physical and virtual environments. These award-winning products come together under the Business Unit’s commitment to a 100% channel business model driven by more than 10,000 partners worldwide.