DynaSis

Disaster Recovery for Business Owners

Practical Guidance for a Critical Operation

April, 2013

Disaster Recovery For Business Owners

Practical Guidance for a Critical Operation

With 57% of small to medium-sized businesses (SMBs) having no formal disaster recovery plan (Symantec, 2011), and 52% believing that computers are not critical to business continuity, it's evident that SMBs don't take the threat of disaster seriously. That's unfortunate, because 45% of SMBs have reported having some type of data loss (Spiceworks, 2013), and one in four will experience a "significant crisis" in any given year, per the Association of Small Business Development Centers.

Consider the role that electronic records play in your business—email, accounting files, customer contact lists—how long could you survive without them? The reality is that some businesses can survive without their business data longer than others. A small minority might even be able to rebuild from scratch with no records. The question then becomes, how much risk—and how long of an outage—can they tolerate? In terms of data recovery, how much are you prepared to lose?

Whether or not you have considered these questions in the past, you should be doing so now. Most SMBs think they lack the time to calculate the possible consequences of an adequate disaster (including data) recovery plan, not to mention the time and funds to implement one.

In reality, most businesses are already losing more in revenue from the day-to-day hassles of downtime and data problems than it costs to implement a disaster recovery solution. In this white paper, we will explore the situation and help you come to terms with the task of creating a workable solution.

The Metrics of Loss

The average data-loss event costs SMBs $9,000 (Spiceworks, 2013) and a major event could cost significantly more. Fortunately, thanks to cloud recovery solutions and the ubiquitous nature of technology, it has become affordable for firms to enact recovery plans that help them avoid exploring their "worst case scenario."

It's also become easier to quantify risk tolerance, thanks to specific metrics that are simple and straightforward. Defining these metrics for your business is the first step to business security and continuity. IT experts describe data recovery in terms of three key metrics:

Recovery Time Objective (RTO): Your goal for the minimum time within which you would like to restore your data, applications and critical IT-related processes after an outage. Would you like to be able to gain instant access, perhaps through a secure portal on the Internet? Or, would you be able to wait a few hours, days or a week to receive a drive image and/or rebuild your system locally or over an Internet connection?

Recovery Point Objective (RPO): The point to which you want your data restored. Many backup solutions create periodic "snapshots." If an outage occurs between snapshots, you will lose everything since that point. Other solutions duplicate your activity as it happens, and in the event of an outage, you lose nothing (or at most, a few seconds). Could you afford to lose an hour's; a day's; a week's worth of data?

Maximum Tolerable Outage (MTO): The longest amount of time your business could be disrupted by loss of access to your data, email and applications before it jeopardized your business continuity and/or client relationships. Any timeframe greater than this is considered a disaster. Calculating your MTO is where you begin to hone in the ROI of disaster recovery preparedness.

What Are Your "Magic" Numbers?

Rather than making a rough guess about your risk tolerance and potential for loss, experts recommend companies gather sufficient intelligence to make an educated projection. We wish we could lead you to a calculator where you could plug in a few numbers and see your MTO and/or potential business loss from a disruption. Such a thing doesn't exist, although there are tools that can help you with this and other information-gathering activities. A good start (and a great resource) is the Business Continuity Planning Suite offered by the Federal Emergency Management Agency on its disaster preparedness site, Ready.gov.

Your potential financial losses will dictate how quickly the business needs to resume—and how much your budget should be for technology to help prevent an outage exceeding that timeframe. Keep in mind as you tally the figures that the average small business loses $55,000 a year in revenue due to downtime, data loss (e.g., corrupted or accidentally overwritten files) and recovery, per Coleman Parkes Research. Mid-sized businesses lose $91,000. That's before any calculations for an actual data disaster.

Business Impact Analysis

Before you can calculate the cost of lost data, you'll need a Business Impact Analysis (BIA). Core steps include:

1. Make a list of core functions and their related data with which you could not continue operating. These include processes crucial to revenue generation, such as sales, as well as any operational activities such as accounting. Critical data will likely include customer and vendor lists, contracts and purchase orders, accounting and other corporate records, and other documents vital to business continuity.

2. Identify the supporting infrastructure for core business operations. You will need at least some of the same (or similar) systems in place before your business can be deemed recovered.

3. Calculate your potential losses from an unplanned interruption. Your accountant should be able to help you peg each critical function to a monetary value- how much money is lost when the revenue stream is interrupted. Calculated losses should include not only lost sales opportunities, but also the loss of customer goodwill, holding expense for excess inventory if you miss sales tied to holidays or other business cycles, and other considerations. The sum of these losses will help you determine how much you should spend to prevent them.

Time Calculations

With this information in hand, you can begin considering the time involved in returning your business to a functioning state. In addition to your own considerations for data needs, speak with your staff to determine how much time they could reasonably lose. You should be able to identify a specific point at which all critical systems must be fully operational for effective, long-term business function.

In today's fast-paced business environment, an increasing number of firms are deciding that no downtime is acceptable. Solutions exist that can free you from time calculations and restraints, enabling you to transition

immediately to a fully operational infrastructure, with your backups intact, from a local or remote location.

Dependencies come into play with downtime calculations, as well. For example, if you suspect your business can tolerate only 48 hours of downtime, you'll need to deduct from that the time to get servers, networks, and other critical infrastructure up, and to load applications and data. You may also come up against procurement issues, personnel availability and other considerations that affect your RTO, RPO and MTO.

While you are making time calculations, consider your RPO. Ask key personnel how much of a lapse, in terms of data lost between backups, they can tolerate. Beyond email and contacts (which are only a piece of the puzzle), consider how your backup frequency might impact customer relationships or damage to your brand. Would you be comfortable asking customers to send you documents that were not backed up before the disaster occurred? In essence, if you opt for infrequent backups (weekly or greater), you are accepting the consequences of a minor data loss.

Risk Assessment

Once you know how much you could lose during a disaster, you must also calculate the likelihood of such an event. This isn't a precise science, but you can figure out your location's likelihood of a natural disaster, tally the approximate number of power outages your area experiences due to weather, and explore your firm's history of data loss. You've probably already weathered one or more minor disasters—and may have employees that can help you quantify it. IT professional are also available to help you determine this.

The Cost of Peace of Mind

Armed with this information, you can begin pricing equipment, backup solutions and outside vendors who can assist you with your recovery efforts. Explore cloud-based backups, which can be updated every few minutes. (Don't forget to ask about recovery time. Some of these solutions will let you recover a few files immediately, but if you want an entire drive image, it can take days.) Price a worst-case scenario where you lose all your hardware and then develop alternate scenarios for lesser problems such as a drive crash or a localized power outage.

Once you've crunched the numbers and calculated the cost of continuity, you can determine the ROI for various backup solutions. The options are myriad, from dedicated, on-premise backup devices that replicate data to the cloud, to hosted backup servers at a best-practices data center. Whatever you decide, don't wait too long to implement a plan. Even a simple plan—one that identifies key activities and personnel to enable low-level functionality—is better than none.

Best Practices for Developing a Disaster Recovery Strategy

- **When you quantify the cost of business continuity, don't forget to include the value of daily continuity.**
- **Downtime is expensive and fairly frequent for many businesses. Disaster recovery plans with short RTOs and RPOs do more than help you recover your business in the event of catastrophe. They can also mitigate the revenue losses from minor outages and data disasters that plague SMBs on a regular basis.**
- **If you are leaning toward zero or very short recovery timeframes, consider moving critical applications to a service provider working under a service-level agreement. Depending on the agreement, you should require little to no recovery strategy for that application.**
- **Not all your critical business applications will have the same RTO, and this will affect your MTO. For example, you might determine that access to email and contacts needs to be nearly immediate, but that RTO for accounting and inventory applications is a few days or more. In this scenario, if your email and contacts data is stored on smartphones or other remote devices, it will meet the core criteria for this data group and allow you to extend your overall RTO.**
- **Don't forget to consider recovery time for an application's own processes. For example, an architect might need to load a terabyte or more of blueprints before he could resume full operation.**
- **Document all your research and calculations for posterity and develop a program for executing the various components of the recovery effort (including assigning tasks to personnel). Share this information with your employees and distill it to its essence for ready reference in the event of a disaster.**
- **Test your backup and recovery processes at least once a year. If you cannot manage testing on your own, hire an IT service provider to do it.**
- **The overall rule of thumb is that the total cost of a recovery strategy should never exceed the losses it is designed to prevent. With that in mind, any number up to that point makes your recovery strategy a profit center.**

DynaSis is a managed IT service provider for small and medium-sized businesses in Atlanta, Georgia. DynaSis specializes in offering on-premise and on-demand managed IT service plans, managed hosting and professional equipment installation. For more information about DynaSis' services visit www.dynasis.com.