



Disaster Recovery: Options for Investment Managers

A White Paper from
Advent Software and CyGem Ltd.

Advent Software, Inc.

This communication is provided by Advent Software, Inc. for informational purposes only and should not be construed as, and does not constitute, legal advice on any matter whatsoever discussed herein.

Table of Contents

Overview	3
How Would a Disaster Affect Your Business?	4
Know Your Risks	4
The Two Key Factors: RTO and RPO	5
Options and Tradeoffs: The Seven Tiers of Disaster Recovery ...	6

From terror attacks to hurricanes, events in recent years have brought the issues of disaster recovery and business continuity into sharp focus for asset managers and broker-dealers—not to mention regulatory bodies, institutional investors and even savvy retail investors.

With rule 206(4) 7, the SEC now requires every investment advisor to adopt and implement written disaster recovery policies and procedures. In their words, the SEC considers it an adviser's obligation to "take steps to protect the clients' interests from being placed at risk as a result of the adviser's inability to provide advisory services after, for example, a natural disaster..." While the SEC recognizes that compliance plans and procedures vary, they have specifically listed business continuity as an area firms must address. In recent audits, examiners have asked firms to provide copies of their disaster recovery plans.

Institutional investment boards and consultants are also asking firms that manage their money—or aspire to—about their disaster recovery capabilities. Managed account program sponsors are making it part of their due diligence process when evaluating potential firms to enter their programs. Individual investors are increasingly aware of and concerned about these issues.

With the increased attention on disaster recovery, asset managers are being compelled to answer tough questions and are often uncertain of where to begin or what is appropriate for them. This document is intended to help asset management firms understand their options. Ultimately the choice of a solution will be based on a firm's size, the nature of its business and how long it can go without client account and transaction data—and, of course, how much the firm is prepared to spend. The information presented here will enable you to have a productive conversation with a disaster recovery consultant or solution vendor, and help you understand the range of options available based on differing needs and budgets.

How Would a Disaster Affect Your Business?

Disaster recovery is an easy issue to push to the side, especially for smaller firms. Often, they barely have enough time to service their clients, research markets and make investment decisions. Why would they take the time or go to the expense to plan for a major site loss when some estimates indicate that it has a less than 2% chance of occurring?

In determining your best course of action, the key factor is not the probability of a disaster, but the impact that a disaster can have if it does happen. The impact depends largely on your specific business. It may not be as important for a buy-and-hold money manager to return to operations as quickly as a hedge fund that trades many times over the course of the day.

Fortunately, the Internet and the decreasing cost of disk drives have made it more affordable for firms of any size to get their data offsite. Once the means of getting data offsite is determined, you then need to determine your restore strategy. Here, too, many options are available for smaller firms, including “quick ship” programs that deliver new hardware in emergencies or agreements with off-site facilities to use their equipment. If a firm has more than one office, it might make sense to house old equipment at a branch office to use in the event of a disaster at headquarters.

Know Your Risks

It does not take an unusually violent act or cataclysm to constitute a disaster. Broken water pipes, a waste-basket fire, electrical surges, computer viruses, office theft and vandalism—these are just some of the everyday threats that can have just as big an impact on an unprepared operation. A basic step in mitigating the impact of a disaster is to identify the vulnerabilities in your office environment.

Most discussions about disaster recovery assume that everything needed to continue operations is already in a digital format. Many organizations, however, still rely on paper such as trade-confirms, brokerage statements and physical checks to run their business. If your firm is relying on non-digital information, you will need to think through ways to either have alternate access or digitize this information.

Besides the potential loss of business-critical data, there are unquantifiable factors, such as adverse publicity or loss of client confidence if you don't have adequate procedures in place—or if you are caught unprepared by a disaster. There's also the matter of publicizing performance. In order to make a performance number claim, you have to have the back-up transaction and account data on file to support it. If you lose that information, you cannot make the claim.

Risk assessment—determining your vulnerabilities and the impact a disaster could have on your business—is the first step in disaster recovery planning. While the likelihood of a disaster may be low, the impact on your business could be large, making some kind of plan preferable to none.

Two Key Factors: RTO and RPO

Before you begin to evaluate technology solutions for disaster recovery, you need to consider two key factors: your recovery time objective (RTO) and recovery point objective (RPO).

RTO is how quickly you need to get your business back in order. If you are a broker dealer and make money by placing trades, you want to get up and running as soon as possible. Every minute that you are not up is costing you. If you are an asset manager and bill on the amount of assets you manage quarterly, a longer RTO may be acceptable. The shorter your RTO, the more your solution is going to cost.

RPO is the point in time to which you need to be able to restore. For example, do you want to recover from one week ago, one day ago or fifteen minutes ago? The further back the RPO is from the present, the less your solution is going to cost. The ability to restore your infrastructure from one week ago will cost less than trying to restore your systems from fifteen minutes ago. A firm that does a lot of trading would probably have a more recent RPO than a firm that trades infrequently. It would take the firm with more trades more time to manually reenter all of their transactions. The more transactions you have, the lower your RPO needs to be in order to minimize the number of transactions that would need to be recreated. For organizations with fewer transactions a higher RPO might be acceptable.

So what are your RTO and RPO? Broker-dealers may have an easier time figuring out the answer. They know the approximate number of trades they are likely to place on any given day. They can then calculate the dollars lost for every day they cannot trade, and determine what they are willing to spend on disaster recovery to ensure that they can keep trading and making money.

A buy-and-hold asset manager may have a more difficult time reaching a conclusion as to how much disaster recovery is worth. They typically get paid in terms of a percentage of the assets they manage and bill quarterly. If they don't trade on a certain day it doesn't necessarily cost them an exact dollar amount. The greater risk is that they may lose clients or be subject to legal or regulatory action if they cannot restore account and transaction data in a timely manner.

Another factor affecting recovery time is the restoration of the system state, namely the part of the computer that contains items like the Operating System and custom settings. If your backup solution addresses only the storage of data, it will take you longer to recover. Many backup systems can back up your system state, which will decrease your recovery time objective, but most require you to have identical hardware to which you would restore. You need to make sure your disaster recovery vendor carries your hardware or provides an alternate means for restoring your system state. Your alternative would be to load new operating system instances on the hardware and then restore your data on top of the new installations. Often, the system state can take significantly longer to restore than the data itself.

Options and Tradeoffs: The Seven Tiers of Disaster Recovery

In 1992 an organization called SHARE (<http://www.share.org>), an independent user group providing IBM customers with services, education and professional networking, created the seven tiers of disaster recovery. As you move from the zero tier to the seventh your recovery time decreases, while your cost or value increases exponentially.

Tier 0: No off-site data—possibly no recovery. You don't have a backup plan so you don't have a recovery. Of course, you save money because you pay nothing for disaster recovery. A disaster, however, could cost you significantly.

Tier 1: Data backup with no hot site. In this scenario, businesses back-up to tape and then have someone take the tape offsite—also known as PTAM or the Pick-up Truck Access Method. This approach suits organizations that can accept days or weeks of data loss knowing their backup data is secure. This tier does not address how the data will be restored in the event of a major data loss.

Tier 2: Data backup with a hot site. This scenario combines tape backup with the ability to restore the data at an alternate facility referred to as a "hot site." The recovery time objective is more predictable than Tier 1, but the recovery point objective is similar to Tier 1 in that you still may need to recreate several days worth of data.

Tier 3: Electronic Vaulting. Instead of relying on PTAM, organizations ship their backup copies offsite electronically. This might mean sending data to a hot site via T1 line or, as is happening more and more, using an online service with no hot site. Using the Internet means you don't have to go to a specific location to run your business—you can run it from virtually anywhere you have Internet access. The recovery point objective is better than that of the lower tiers as there are fewer transactions to recreate.

Tier 4: Point-in-time copies. This is a plan that accounts not only for data, but also for the exact system state to reduce the amount of time necessary to recover systems. At this tier, companies begin using disk-based or online backup, which is easier than backing to tape and can be done more frequently. With an enterprise backup provider, software is installed that takes a snapshot of a firm's entire system. The data is sent off site and the firm can recover its entire system to new and different hardware.

For small- to mid-size investment managers, Tier 4 is the minimum recommended level of disaster recovery readiness. In balancing dollars spent and protection gained, it allows for secure offsite vaulting without going to the expense of a full disaster recovery facility. Solutions at this level are relatively easy to use, and therefore are more likely to be used, especially in firms with minimal or no IT staff. You can be confident that your data is secure and your firm is protected without relying on someone to manage the backup and tapes that accompany it.

In comparing online services, which often have wildly differing prices, it's important to recognize the distinction between workstation backup and server backup. Workstation backup is less expensive, but if you are in a SQL environment you will need a server-based backup solution.

Tier 5: Transaction integrity. Sometimes referred to as "host-based replication," solutions at this level involve having identical data at two facilities, one primary and one secondary. This is achieved by installing data-mirroring software onto the operating system. The software replicates the data between the two sites, so there is no data loss in the event of a disaster at either site.

Tier 6: Zero or near-zero data loss. Similar to tier 5, with the exception that replication is no longer provided by an application on the operating system at the host level. It occurs on the storage platform itself. An example is SAN (storage area network) -based replication. For enterprises using multiple operating systems, SAN-based replication simplifies the process because it is independent of operating systems.

Tier 7: Highly automated, business integrated solution. In this tier replication and failover happen automatically among multiple servers at multiple locations.

Solutions at Tiers 5, 6 and 7 are geared to large organizations with multiple locations, high transaction volume and tens of billions in assets under management. At 6 and 7 in particular, the cost is going to be very high with the tradeoff that not a single transaction will be lost.

Deciding what RTO, RPO and tier are appropriate for your organization is not a simple task. It takes business knowledge combined with the ability to find vendors able to deliver solutions that are appropriate for your organization and budget.

Whatever solution and tier you decide to use, make sure you test with your environment. No two organizations are the same. Even if a vendor claims a 100% success rate, it is important to understand exactly what that 100% means. You should also plan to re-test as your organization and systems go through changes.

Geoffrey F. Moore is a managing partner with CyGem, Ltd., specializing in managed hosting and disaster recovery services. Prior to CyGem, Ltd., Mr. Moore worked for Oak Associates, a large-cap growth money manager, in operations and information technology.

About Advent Software

Advent Software, Inc., a multi-national company, has provided trusted solutions to the world's leading financial professionals since 1983. Firms in more than 60 countries using Advent technology manage investments totaling more than US \$12 trillion. Advent's quality software, data and services enable financial professionals to improve service and communication to their customers, allowing them to grow their business while controlling costs. Advent is the only financial services software company to be awarded the Support Center Practices certificate for being a world-class support organization.



Advent Software, Inc.

600 Townsend Street, San Francisco, CA 94103
800-727-0605 415-543-7696

666 Third Avenue, New York, NY 10017
212-398-1188

www.advent.com

Copyright © 2006 Advent Software, Inc. All rights reserved.