

# Disaster Recovery Strategies for Hedge Fund Managers

## *Issues and Considerations*

### **About Eze Castle Integration**

Eze Castle Integration ([www.eci.com](http://www.eci.com)) is the leading provider of outsourced IT services to the investment industry. The company's service areas include Startup and Relocation, Outsourced Technology Support, Telecommunications, Business Continuity Planning and Archiving, and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in New York, San Francisco, Minneapolis, and Greenwich, CT.

# Table of Contents

<b>Expect the Unexpected</b> .....	3
<b>Disaster Recovery Issues and Challenges</b> .....	4
Capital Costs – What’s The Right Economic Choice?.....	4
Data Protection – Tape Is Not Enough .....	4
Outsourcing: Avoiding the Distraction Factor.....	5
<b>Defining the Right Objectives for Your Hedge Fund’s DR Plan</b> .....	6
Hot Sites vs. Remote Sites: The Trade-Offs.....	7
Redundant Infrastructure.....	8
Security.....	9
Testing.....	9
<b>Eze Castle Integration Business Continuity Services</b> .....	10
<b>A Quick Checklist for Your Disaster Recovery Plan</b> .....	11
<b>Conclusion</b> .....	10

## EXPECT THE UNEXPECTED

In the high-pressure and high-stakes world of hedge funds, a business interruption can quickly become a business killer. With their complete reliance on a sophisticated foundation of powerful computers and applications, data networks, and voice communications, hedge funds cannot afford even the slightest disruption in their IT service.

When we think about disaster recovery strategies, most of us envision natural disasters, such as floods, tornados, hurricanes, and earthquakes. However, a better definition encompasses *any* event that prevents you from accessing the data and systems you need to conduct business. That could be a regional power failure or a rapidly spreading computer virus. It could also be employee sabotage, external data fraud, devastating terrorist attacks, or even an influenza pandemic.

Regardless of the cause, there's no room for outages, especially when, according to analyst firm Gartner, downtime can cost a financial institution up to a staggering \$1 million an hour. Consider the impact if your trading systems go down. Or your voice-communications are disrupted during crucial trading hours. For hedge funds pursuing sophisticated strategies that rely on the ability to detect and exploit short-lived inefficiencies and opportunities, those interruptions are extremely costly.

The damaging implications of these disasters are plainly evident. According to analyst firm Infonetics, the average financial institution experiences 1,180 hours of downtime per year, costing them 16 percent of their annual revenue. Given the stakes, most companies believe that disaster recovery planning and preparedness are non-negotiable requirements.

With so much at stake, your company has no option but to implement a sophisticated disaster recovery plan. In their routine pre-investment due diligence audits, your investors will expect that a comprehensive, tested disaster recovery plan is in place. And, now as a Registered Investment Advisor with a fiduciary responsibility to clients, a DR plan not only the smart strategy, it's an SEC requirement as well.

## THE DISASTER RECOVERY ISSUES AND CHALLENGES

For many hedge funds, disaster recovery remains an Achilles heel – an expensive and sometimes distracting proposition and a discipline requiring specialized talents that are often difficult to recruit and retain. Consider some of the many hurdles for disaster recovery in hedge funds.

### **Capital Costs – What’s The Right Economic Choice?**

Every hedge fund’s business-specific requirements will vary. Some adopt buy-and-hold “long” strategies that have fewer trading requirements. Others pursue technical and sophisticated strategies to exploit inefficiencies, requiring fast, high-volume trades. Your disaster recovery preparations and strategies must reflect those underlying business requirements, which will in turn directly shape your capital-budget decisions.

You will need to devote funds for server hardware, software, connectivity, and other resources and train your staff. Collectively, these represent major investments of capital. More broadly, you must consider if outsourcing disaster recovery to a service provider or keeping it in-house is right for your business. As you evaluate in-house versus outsourcing additional questions to consider include “should you lease the real-estate and procure, install, and maintain all of that equipment yourself?” and “what are the capital-budget implications of outsourcing DR versus handling it in-house?” Regardless of the approach, a disaster recovery strategy should include either a hot or remote site that replicates your current IT environment and enable your workers to be up and running immediately in the event of an outage.

In general, the upfront capital costs of each in-sourcing vs. outsourcing approach are roughly equal – but ongoing maintenance and management may be higher with different approaches and should be given careful consideration.

### **Data Protection – Tape Is Not Enough**

One of the most important issues in business continuity is protecting your most crucial asset: data. Your data is too valuable to strictly rely on unstructured backup and archiving processes with unreliable media. For many companies, tape is the attractive medium because of its low cost -- and it’s an appropriate choice for day-to-day restoration, archiving or longer-term storage.

However, with the many challenges that it presents, tape is completely unsuited to the critical tasks involved in disaster recovery and business continuity.

Consider some of the uncertainties that come with tape:

- Have you captured a good, valid backup? Is there data on the tape?
- Where are you storing the data? If it isn't offsite, the backup may not be helpful if your data center is destroyed.
- Are the drives and equipment at the offsite location compatible with your tape format?
- Assuming you have compatible systems, will the tapes index and restore correctly to achieve a successful recovery?
- How quickly can you access the data on the tape and become operational?

For these and many other reasons, many hedge funds are increasingly turning from tape to online backup. With online backup, the data can be captured on a continuous or near-real-time basis to a remote facility. The backups are more reliable than notoriously unreliable tape, especially considering as many as half of all tape restores fail.

### **Outsourcing: Avoiding the Distraction Factor**

The time you devote to planning, implementing, and testing your disaster recovery plans and infrastructure is, of course, well-spent should disaster strike. However, it's inescapably true that disaster recovery planning and management can be a major distraction from your core goals: managing investments. While the potential returns and savings from a DR system are vast, firms make the most money focusing on what they do best.

Understandably, most firms are reluctant, at best, to invest the time required to understand, execute, and manage a thoughtful, comprehensive DR plan, preferring instead to devote their time to the revenue-generating activities of the firm. They want to concentrate on trading strategies and investment opportunities, however, a DR system is a critical component of any responsible investment firm.

The alternative is outsourcing appropriate portions of the disaster recovery plan to qualified service providers who can bring infrastructure, expertise, and focus to your DR requirements and challenges.

## DEFINING THE RIGHT OBJECTIVES FOR YOUR HEDGE FUND'S DR PLAN

One of the first steps you need to take as you formulate your disaster recovery strategy is to prioritize all of your critical systems and make thoughtful “triage”-style assessments about what data, application, and voice systems are most important. One of the key metrics in this process is determining the Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for various applications, systems and data sources.

An RPO is the targeted point in time to which systems and data must be recovered after an outage and represents the maximum amount of data loss a business can incur in an outage. Organizations must first determine their RPO and then build a DR application that meets that RPO.

For example, a trading application might have an RPO of 30 seconds. Only the most recent 30 seconds of data would be unavailable in the event of an outage and recovery. An e-mail server might have an RPO of four hours. And the company's static Web site might have an RPO of 24 hours.

The RTO is the goal for the amount of time it takes to actually recover that lost data or service. In other words, how long are you willing to wait? The RTO for mission-critical systems – such as trading or voice systems might be extremely short – while the RTO for a general ledger system might be several hours. These choices carry significant implications in terms of the investments they require, so you need to carefully analyze the various tradeoffs to make the right choices for your firm.

Even your trading strategies can affect these decisions. For example, if your firm is primarily going along with a buy-and-hold strategies, your RTOs might be longer than a firm engaged in high-complexity arbitrage or sophisticated quant strategies.

Another consideration is to factor in the “key contributor” dimension. Ensure that your key contributors receive added emphasis and attention in the DR plan so that your biggest revenue-producers (or, perhaps, portfolio managers) receive higher priority for service restoration.

## Hot Sites vs. Remote Sites: The Trade-Offs

A hot site is a remote physical location where you can maintain copies of all of your critical systems, such as trading applications, and data, which is perhaps backed up onto disks through the online means just discussed. The hot site also encompasses real estate with separate offices, cubes, desks, workstations, laptops and other office resources and infrastructure (e.g. phones, copying machines or printers) that people can use to work alongside one another much as they do pre-disaster.

Of course, for a hot site to be most useful, your people will need to be able to access it quickly. That implies it would be located in reasonable proximity to your primary location. However a hot site that's close enough for employees to reach may be too close. A natural disaster such as a hurricane or earthquake could cut a wide swath and put *both* locations out of commission. However, if the hot site is too far away, your employees may not be interested in driving 50-100 miles to reach it – especially at a time of a natural disaster or unrest that leaves their home or family vulnerable.

It's important to understand that operators of these hot sites “overbook” their facilities. Much like airlines, these facilities charge on a per-seat basis and overbook their seats to maximize their profit. In the event of a widespread crisis, you may find yourself competing with other hot site customers for the same facilities. Make sure you understand your rights and access privileges.

By contrast, a remote site provides a more focused and efficient set of services that may be entirely more appropriate for a hedge fund. A remote site provides a replica of your IT environment – without physical desks and office infrastructure – that you and your firm's employees can securely access and use through standard Internet connections from anywhere. In most cases, this model provides several advantages:

- **Lower Cost** – You don't pay for office, real-estate, or telecommunications overhead because your employees access it from their preferred remote location such as their homes or one of your branch offices.
- **Assured Access to Dedicated IT Resources** – Instead of worrying about competing with other hot site clients for limited space and resources, you can access dedicated IT resources housed and professionally managed at the remote site.

- **Greater Convenience for Employees** – Your team doesn't need to be concerned with traveling great distances under trying circumstances. An effective business continuity plan includes contingencies for multiple types of outages, so locking your employees into meeting at, or working from, one location can reduce the plan's effectiveness – adaptability is key.

Regardless of which model best fits your business's requirements, there are three important factors to include in your evaluation/selection process: Infrastructure, Security, and Testing.

### **Redundant Infrastructure**

The infrastructure of the remote site or hot site must have multiple levels of redundancy designed and built into every aspect of the facility.

- **Network** – Make sure your provider has redundant network equipment and multiple service providers.
- **Power** – There should be multiple sources – perhaps even sourced from different power grids – as well as backup power generators and on-site fuel to run those generators.
- **Air Conditioning** – Servers and other systems generate a significant amount of heat, making backup cooling systems a key component of a DR facility.
- **Security** – For data and telecomm, your DR partner should deploy an uncompromisingly high level of security through technologies such as virtual private networks (VPNs), virtual LANs, firewalls, and more.
- **Redundant Systems** – Whether it's servers, routers, or T1 lines, your remote site or hot site provider should have "N+1 availability" where – like a spare tire - there's always one additional spare that can be deployed if a primary unit fails.
- **Storage** – The best deployments use RAID methodologies to "stripe" data across systems for performance and mirror that data for improved protection and availability.
- **Application Software** – Ideally, your remote-site provider can accommodate multiple strategies, including redundancy, clustering, load-balancing, and warm-standby (where the application is loaded but not running).

## Security

From a facilities standpoint, you want your remote site to have an even higher standard of physical security than your primary data center – since those sites have a constant flow of people often times unaffiliated with your company. Important must haves include:

- Locked cabinets, cages, and rooms housing your equipment
- Human security, including guards monitoring video cameras, patrolling and managing visitor logs
- Biometric security
- Perimeter/monitoring security

## Testing

A disaster recovery plan is only useful if it's regularly and rigorously tested. When an outage strikes, you don't want to rely on an untested DR plan, only to find gaps, mistakes, and failures that leave you without service. Regular testing allows you to find and amend gaps caused by technology changes or upgrades, while training your employees on best practices so they are comfortable when the DR plan is executed.

The key to testing is to start off small and then build to a full, comprehensive test that includes an unannounced exercise. By starting small, employees become aware of, and comfortable with, the resources available to them during an outage. Tests should be led by individuals with background and training in DR solutions, as testing requires the shutdown of various systems and components to ensure appropriate failovers occur. A few essential plan testing guidelines include:

- Provide detailed procedures to employees and closely follow them during a test
- Verify the backup data and telephone trees
- Testing should involve actual data
- Change the scenario from test to test

## The Six Facets of Comprehensive Disaster Recovery Plans

- **People** – Without people, your DR plan has no traction. How will you notify, evacuate, transport, house, feed and care for employees? How will you pay them?
- **Property** – What kind of work environment will your people require? Can they telecommute or do you need alternate "hot-site" office space?
- **Systems** – What components of your telecomm and computing infrastructure must be ready immediately? Do you have backup hardware and software ready to put into service?
- **Data** – What data is critical to run your business – and how will you recover any critical data that's lost in the disaster?
- **Recovery Time Objective** – How quickly must you have your company's IT systems available? Is that in a minute, an hour, or a day?
- **Recovery Point Objective** – For each system, determine how much of your data can you afford to lose in an outage. If it's a trading transaction system, the answer might be none. If it's an e-mail server, perhaps the answer is 30 minutes.

## EZE CASTLE INTEGRATION BUSINESS CONTINUITY SERVICES

With more than a decade of experience, Eze Castle Integration has the track record, expertise, and resources to help financial services firms capitalize on the power of IT for business gain. The company's Eze Business Continuity Portfolio features a full-range of managed IT and consulting services to help clients ensure their critical information and systems are protected and always available. The Eze Business Continuity team boasts more than 70 years of data protection experience and includes Certified Business Continuity Professionals (CBCP).

The company's flagship IT Business Continuity offering, Eze Disaster Recovery Services (Eze DR) works by replicating mission-critical data to remote, fully redundant data centers outside the geographic region of a client's primary location. When an outage occurs, any authorized employee can access the data and applications using an Internet connection from virtually anywhere. To accommodate a broad range of client requirements, Eze Castle Integration offers three levels of disaster recovery and high availability services: Eze DR Silver, Eze DR Gold and Eze DR Platinum.

- **Eze DR Silver** is ideal for firms seeking a cost-effective data protection solution with a rapid "go live" time. With Eze Castle Integration's Quick-Start feature, protection of critical data can begin within 10 business days from the start of the agreement.
- **Eze DR Gold** provides high availability and disaster recovery for business-critical data and applications. This service is ideal for firms that rely on critical applications, such as order management systems, Microsoft Exchange, or in-house systems, to operate their businesses.
- **Eze DR Platinum** gives firms the optimum disaster recovery and high availability solution with real-time data replication, application availability, near-zero downtime, and innovative technologies such as storage area networks.

## CONCLUSION

In most instances, fortunately, business continuity incidents revolve around relatively mundane matters such as a local power failure or a water-main break. However, that doesn't mean their damage can't be detrimental or potentially fatal to your business. With careful analysis and planning, you can prepare to "expect the unexpected" and ensure your firm can continue business as usual operations in the event of an outage. For more information, visit [www.eci.com](http://www.eci.com) or call 800-752-1382.

### A Quick Checklist for Your Disaster Recovery Plan

- ✓ Analyze voice, data systems and determine RPOs and RTOs for each system
- ✓ Classify each into prioritized categories
- ✓ Identify key performers requiring earliest access
- ✓ Identify remote-site provider candidates
- ✓ Establish service level agreements (SLAs) with service providers
- ✓ Evaluate the quality of the provider's infrastructure
- ✓ Assess the provider's data/voice and physical facility security
- ✓ Assess the provider's testing plans