Establishing Business Continuity and Disaster Recovery Plans

A Hedge Fund Manager's Guide

Our partner in developing this guidebook:

EzeCastle INTEGRATION

Pershing® Prime Services
A BNY MELLON SERVICE

Contents

Introduction

In the past, firms only needed to plan for, and protect themselves against, events such as fires, hurricanes, tornadoes, earthquakes, floods, power failures and communication outages. These are statistically predictable, quantifiable, insurable and well-understood events. Today, firms must also consider events that are intentional, difficult to quantify, have ambiguous boundaries and involve dimensions of trust—events such as cybercrime and denial-of-service attacks; terrorist targets of opportunity; wireless devices; trading partner connectivity; public infrastructure concerns, such as telecommunications, airlines and globalization; and protection of human capital.

Studies show that businesses lose an average of about $5,000 per minute in an outage, and for financial firms the losses are typically even greater. At that rate, unplanned downtime of critical systems could cost a large company as much as $300,000 per hour or greater due to lost revenue, reduced employee productivity and possible regulatory penalties. Those figures do not include the negative impact on the business' reputation.[1]

Additionally, other key influences that are driving businesses to manage risk by creating business continuity and disaster recovery plans include:

- Investors becoming more stringent in vetting a firm's business and information technology (IT) practices as part of the due diligence process, particularly around disaster recovery and business continuance
- Regulations requiring that funds have business continuity and disaster recovery plans and procedures in place
- Development and implementation of industry best practices

As a result, hedge funds are proactively creating plans and procedures—before investors request them—and taking every reasonable step necessary to protect their clients' investments and help ensure that they meet fiduciary responsibilities.

Purpose of the Guide

This guide is aimed at helping hedge fund managers of various size funds develop an understanding of both the business continuity and disaster recovery planning processes and their underlying principles.

- Business continuity and disaster recovery plans must consider a wide range of events and how they will affect each level of the firm and its business. Any possible risk must be identified and analyzed in order to design effective business continuity and disaster recovery plans. The appropriate solutions take into account the hedge fund's specific needs and systems, as well as the manner and environment in which the fund operates.

- Effective business continuity and disaster recovery plans seek to achieve two results. First, provide an understanding of which procedures and personnel are essential. Second, address documenting, planning, implementing, testing and maintaining the policies, procedures and infrastructure to ensure that mission-critical processes and essential personnel can continue to operate or quickly return to operations after an unexpected outage. [2]

- Care needs to be given to make each plan as simple as possible. Plans that are too complex or expensive to properly maintain, train on and test, are worse than plans that only perform minimal procedures because they provide a false sense of security.

- Creating effective business continuity and disaster recovery plans may take as long as two to three months or more. The complexity of the planning efforts and the finalized plans will, at the very least, mirror the complexity of the hedge fund's processes and functionality that must be recovered in a short period of time.

It is our hope that this guidebook will provide a framework of important considerations, knowledge and resources to help you make informed business decisions when determining the appropriate business continuity and disaster recovery plans for your hedge fund.

Business Continuity Plans versus Disaster Recovery Plans

A business continuity plan focuses on development, planning and testing of the infrastructure plan developed to address the people, operational processes and business aspects of surviving an outage, primarily:

- What are the mission-critical processes?
- How quickly can they be restored?
- Who are the key personnel?
- How are they going to be notified of an emergency?
- Where and how will they continue to operate?

A disaster recovery plan encompasses the steps taken to implement and support the firm's infrastructure, including hardware, software and sites necessary for the recovery of mission-critical services and applications

such as email, trading, voice, file server, accounting and mobility.

Figure 1 illustrates the different layers of a business and where and how disaster recovery and business continuity planning fit overall.

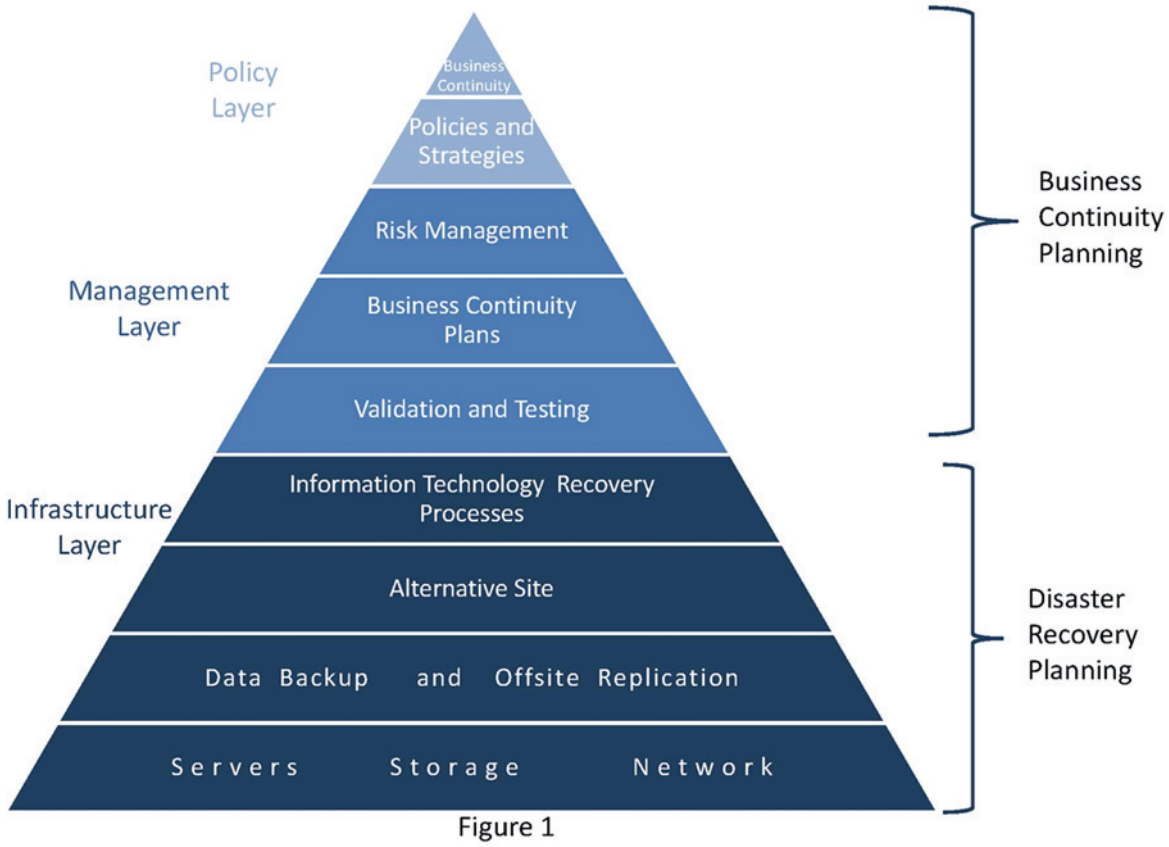

Figure 1

Developing Your Business Continuity Plan

Business continuity planning makes use of the infrastructure addressed in the disaster recovery plan while addressing fundamental operating concerns, as well as personnel planning, in order to minimize the effect of any unplanned downtime.

The primary objectives of a business continuity plan are to minimize potential financial loss, allow for continued service to clients and partners, and diminish negative effects of disruptions on a firm's strategic plans, operations, market position, and reputation. There are two approaches to creating the plan: outsourcing or handling in-house.

Key Considerations When Outsourcing Plan Development

Creating a business continuity plan is a time-intensive process that can often take several months. It involves interviewing the necessary parties, analyzing the collected information, creating multiple drafts of the plan and testing and maintaining the finished plan. As with disaster recovery planning, only experience allows a business continuity planner to fully understand the nuances and interdependencies that ensure a plan will best protect a hedge fund's essential operations and personnel.

Most hedge funds elect to hire a third party to assist with the development, implementation and ongoing maintenance of the firm's business continuity plan. Hiring a third party raises some key issues for consideration:

- **Industry-centricity.** As in any relationship, make sure that the vendor has specific industry knowledge and confirm that it understands your needs and the manner and environment in which you operate. A business continuity plan can then be created that is both customized to match the current size and complexity of your firm and allows for future growth.

- **Certified consultants.** Confirm that the third party uses certified consultants. Uncertified consultants potentially lacking professional competence may deliver a business continuity plan that does not address all your firm's needs or is biased, leading you to purchase unnecessary software or solutions.

- **Complete solution.** The creation of the business continuity plan is only the first step in your hedge fund's contingency strategy. In order to protect your dynamic firm, the plan must change with your firm—maintenance and training sessions ensure that the business continuity plan remains effective and clearly understood by all.

- **Customized and proven solution.** A proven methodology will provide a solution that has been fully tested and vetted in the "real world." In order to be effective, a business continuity plan needs to take into account your firm's specific needs, systems and operating environment.

Key Considerations for Developing a Business Continuity Plan In-House

Business continuity plans must consider a wide range of events and how they will affect each level of the hedge fund and its business. A plan, for example, must consider the potential for wide-area disasters that result in the loss or inaccessibility of office facilities or staff. Plans must also consider geographic, as well as market-based, interdependencies among investment firms and their service providers.

A comprehensive business continuity planning approach covers the four steps of a complete life cycle:

- **Identify**—risk assessment
- **Analyze**—business impact analysis
- **Design and Execute**—strategy selection, plan development and implementation
- **Measure**—plan testing, training and maintenance

The first step of any business continuity plan is to gain your firm's senior management buy-in for development of the plan, as management is ultimately responsible for identifying, evaluating, ranking, overseeing and controlling risks.

The effectiveness of a business continuity plan depends, in part, on management's ability to detail business workflows and commit to maintaining and acting in accordance with the plan. Management's responsibilities include:

- Assigning resources and personnel to develop the business continuity plan
- Establishing guidelines on how the hedge fund will manage and control identified risks
- Supporting, reviewing and signing-off on business continuity plan exercise results
- Reviewing and approving updates to the business continuity plan on a bi-annual basis
- Ensuring employees are trained and know their role in plan execution

Identify Risk

Once executive buy-in has been achieved, the next step is conducting a risk assessment, an outside-in approach to assessing the physical office locations and surrounding areas. A risk assessment helps a firm prioritize potential business disruptions based on severity and the likelihood of occurrence. Threats can take many forms, from natural and man-made disasters to sinister activity. Risk assessment activities should identify all risks and then hone in on the realistic threats.

A threat scenario should reflect the likelihood of the potential event occurring, as well as the potential disruption it could cause. There is an extensive range of internal and external threats that can impact an organization. However, the threat's severity, combined with the probability of occurrence, requires that threats be segmented. A threat such as an earthquake or a terrorist attack may have a high level of severity, but a low probability of occurring. By identifying the high-probability threats, such as power outages, a firm can devise a targeted

business continuity plan that hones in on real scenarios. A plan that is too broad may prove overly cumbersome to test and implement, while a plan that is too basic may omit important steps that could improve business resilience.

Risk assessment helps determine what an actual threat is and will allow for the beginnings of the development of a comprehensive, step-by-step plan.

The basic premise of a business continuity plan and disaster recovery system is to minimize or, in some cases, reduce to zero the time (T) you are down.

A simple formula for estimating the financial risk associated with a given type of disaster, and thus how much it is worth investing in, for a plan to mitigate that risk, is:

$$\text{Risk (\$)} = P \times C \times T$$

P is the probability that the disaster will occur; C is the cost of downtime in lost productivity and lost revenue, among other factors; and T is the time that systems are expected to be down.

For example, if the probability of a major hurricane hitting your place of business in the next three years is 20 percent, and it will cost you roughly $200,000 for every day that you are down, and you expect that you are likely to be down for a week, then your financial risk is 0.2 x $200,000 x 7 = $280,000.

Risk can also be reduced by minimizing the probability that the disaster will occur or by decreasing the cost that will be incurred if it does. This is accomplished by taking preventative measures, which often costs less to implement than the cost of fixing it after the fact. Preventative measures can include:

- Ensuring regular maintenance is performed on critical systems
- Implementing redundant components
- Installing environmental monitoring solutions
- Automatically monitoring the infrastructure to quickly address malfunctions
- Reducing your firm's dependence on the system
- Physically moving the organization to areas not affected by the specified threat (e.g., hurricanes or floods)

Analyze Business Impact

The objective of a business impact analysis is to collect information on a wide range of areas, from recovery assumptions and critical business processes to interdependencies and critical staff. The business impact analysis phase identifies the maximum amount of downtime critical business processes can withstand, as well as the associated recovery point objectives and recovery time objectives. During this phase, your firm should set recovery priorities for business processes and identify essential personnel, technologies, facilities, communications systems, vital records and critical data.

To facilitate this process, one-on-one interviews should be conducted with key business function leaders from all facets of the firm, from trade processing and settlement to human resources. It is important that the business continuity planner follows uniform interview and survey questions during this phase to help ensure consistency of the information collected. Via these interviews, all your hedge fund's processes, systems or resources (e.g., personnel) are considered on an independent level: separate from other processes; systems or resources that depend on them, as well as from other processes; and systems or resources on which they depend.

For each process, system or resource, the following key questions should be answered:

- What are the availability and performance requirements? What is the cost if these requirements are not met?
- What interdependencies exist between current and potential processes, systems and resources?

DESIGN AND EXECUTE A BUSINESS CONTINUITY PLAN

With the risk assessment and business impact analysis information collected, the next phase is streamlining the business function recoverability ratings and threat findings and presenting the information to management for executive sign-off.

Securing executive buy-in for the findings, which will dictate the direction of the plan, is critical. As part of this phase, critical applications are defined and the application architectures are reviewed to identify application availability and recoverability and to address any gaps in the plan.

Development centers on addressing likely threat scenarios, and business operation priorities may require that multiple unique plans are developed for different departments, divisions or office locations. It is here that you do the core work of balancing costs and benefits of the available approaches. This activity is used to lay out the step-by-step plans for recovery under various scenarios, the types of solutions they will entail and to determine the costs involved.

During this phase there are two key considerations. The first is to consider exactly what types of outages you need to prepare for and to classify them by the extent and type of impact they have—the recovery strategies available to you necessarily depend on that from which you must recover. The second consideration is the need for solutions for differing breadths of coverage. Implementing alternative solutions provides a greater level of flexibility.

Keep in mind that systems are not independent of one another and most often require that the recovery strategies be compatible. While a minor consideration for purely local solutions, if you wish to set up an alternate site, you need to ensure that all the systems on which a given system depends are also duplicated. With the development of the plan completed, another meeting should be held to review the output with senior management for sign-off.

Following sign-off, employee review and testing sessions should be held so that key stakeholders become well versed on the plan. However, the implementation of a business continuity plan is only the first step. In order for it to be truly reflective of your firm's environment, and most effective, it is a never-ending process of modification, maintenance, training and testing.

Plan Testing, Training and Maintenance

Business continuity exercises are an essential, ongoing initiative. Your plan must be regularly tested using predefined strategies, which detail the conditions and frequency for testing applications, business functions and supporting information processing. The testing strategy should include testing objectives and associated measurement metrics, scenario scripts and test schedules.

There are many different types and levels of testing, but they will generally span two key dimensions: scope and realism. Scope refers to the extent to which you are testing a full system or just individual components. Realism refers to the degree to which you are performing exactly the procedures that you would perform during a disaster. In practice, the less realism there is in a test, the less intrusive it will be.

A full test should be completed at least once a year, with less disruptive testing of subcomponents performed throughout the year. If a certain part or system that is to be tested depends upon another part, then both should be tested at the same time. This will allow for a full understanding of interdependencies, and produce realistic

tests in order to reduce the potential that people will freeze or an unanticipated event may occur in a real emergency.

Proper training is vital. Procedures in training should be considered part of the regular new hire orientation if they have any role in implementing the plan. Key personnel should undergo training frequently enough that they are intimately familiar with the procedures that they will have to carry out under the plan.

Finally, business continuity plans are living documents that must be updated, at a minimum, of every six months to help ensure that they account for changes within your firm, as well as evolving threat scenarios. As part of the maintenance process, your firm must conduct annual comprehensive business impact analyses or risk having an outdated plan that does not appropriately map to and protect your firm's business recoverability requirements. It is important the plan that is developed accurately reflects the most current requirements and environment.

DEVELOPING YOUR DISASTER RECOVERY PLAN

When most of us think about disaster recovery strategies, we envision natural disasters such as floods, tornados, hurricanes and earthquakes. However, a more complete definition encompasses any event that prevents access to data and systems needed 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, a devastating terrorist attack or an influenza pandemic. Regardless of the cause, there is no room for an outage of any kind as you conduct your daily business operations. Consider the impact of your trading systems going down, or a disruption in voice communications during crucial trading hours.

In the high-pressure, high-stakes world of hedge funds that pursue sophisticated strategies relying on the ability to detect and exploit short-lived inefficiencies and opportunities, a business interruption can quickly become a revenue killer. Because so much of building and maintaining a hedge fund relies on a sophisticated foundation of powerful computers, applications, data networks and voice communications, firms cannot afford even a minor disruption to their IT service.

The President's Working Group, created to provide guidance to hedge funds, states that "to mitigate financial loss in the event of disaster or other business disruption, the manager should establish a comprehensive business continuity and disaster recovery plan." If the fund is a registered investment advisor with fiduciary responsibilities to clients, a disaster recovery plan is not only the smart strategy, but a requirement of the Securities and Exchange Commission.[3]

Defining the Appropriate Objectives for your Hedge Fund's Disaster Recovery 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 which data, application and voice systems are most important. One of the key metrics in this process is determining the recovery point and recovery time objectives for various applications, systems and data sources.

A recovery point objective 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 recovery point objectives and then build a disaster recovery solution that meets those objectives. For example, a trading application might have a recovery point objective of 30 seconds. Only the most recent 30 seconds of data would be unavailable in the event of an outage and recovery. Conversely, an email server might have a recovery point objective of four hours, while the company's static web site recovery point objective may be 24 hours.

The recovery time objective is the goal for the amount of time it would take to recover lost data or service. The recovery time objective for mission-critical systems—such as trading or voice systems—might be extremely short or nonexistent, while the recovery time objective 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 trade-offs to make the right decisions for your firm.

Even your trading strategies can affect these decisions. For example, if your hedge fund is primarily long-only, your recovery time objectives might be longer than those of a firm engaged in high-complexity arbitrage or quant strategies.

You should also factor in the "key contributor" dimension. Ensure that your key contributors receive added emphasis and attention in the disaster recovery plan, ensuring that your biggest revenue producers receive the highest priority for service restoration.

Key Considerations When Building Your Disaster Recovery Plan

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. Many hurdles exist for disaster recovery in hedge funds; however, planning for and taking the right steps to develop a comprehensive disaster recovery plan that is customized for your unique needs will allow you to be best prepared for unexpected events.

There are several steps and considerations you should take into account when mapping out your planned disaster recovery response.

Capital Costs: What is the Right Economic Choice?

Every hedge fund's business-specific requirements will vary. Some funds use a long-only strategy that has fewer trading requirements. Others pursue technical and sophisticated strategies to exploit inefficiencies, requiring fast, high-volume trades. Your hedge fund's disaster recovery preparations and strategies must reflect those underlying business requirements which will directly shape your capital-budget decisions.

You will need to devote budget resources to server hardware or virtualization technology (depending on your infrastructure approach), software, connectivity, other resources and training. Collectively, these represent major investments of capital. More broadly, you should consider if outsourcing disaster recovery to a service provider or keeping it in house is right for your business. As you make this evaluation, additional considerations include potentially leasing the real estate and procuring, installing and maintaining all of the equipment yourself, and determining the capital budget implications of outsourcing disaster recovery versus handling it in house.

Regardless of the approach, a disaster recovery strategy should include remote access to a secondary DR environment that replicates your primary environment and enables your workers to be immediately operational and productive in the event of an outage.

Historically, the up-front capital costs of each in-sourcing versus outsourcing approach have been roughly equal—but ongoing maintenance and management may be higher depending on your firm's individual approach and should be given careful consideration. Cloud delivered disaster recovery services are changing the economics and have the potential to reduce upfront capital costs significantly.

Technology: Evolving Solutions for Data Security

Hedge funds are increasingly turning from tape to comprehensive solutions that will ensure that data are replicated and stored in secure offsite locations, be it the firm's disaster recovery site or a site operated by a third-party vendor.

Offsite data replication includes solutions ranging from online backup to "near real-time" data mirroring. As with a disaster recovery plan, not every solution is appropriate for every firm. Your hedge fund should understand what each solution provides, as it relates to your firm's size and complexity, and the solution's cost.

With online backup, the data can be replicated to the remote facility on a fixed schedule (e.g., once per day or continuously, at set intervals, throughout the day). Online backup ensures that the data is automatically sent to a secure offsite location and retained for a set period of time, stretching anywhere from several days to several years. Also, online backup usually only replicates the changes in data after the entire data store is initially replicated. Online backup is also more reliable than notoriously undependable tapes, especially considering that as many as half of all tape restores fail.

However, online backup also has several factors that must be considered. Typically, online backup is priced based upon the amount of data protected and the length of the retention. As increasingly more data is stored for longer periods of times, the benefits of online backup can be diminished by a cost that greatly exceeds the relatively inexpensive tape solution.

With this in mind, many firms are adopting a hybrid approach, whereby data required for short retention periods is replicated to an online solution—for example, 30 days—and data destined for longer archiving is saved to tape and stored offsite.

Online backups do not make hot-spare servers available. If and when a server fails, or the production environment becomes unavailable, a process should be established to have a spare server available, or to have a new server

built and replicate all the appropriate data stored online to the new or spare server before functionality can be restored.

The concept of data mirroring provides for the "near real-time" replication of data, typically via software or a storage sub-system and a high-bandwidth connection.

Data mirroring can be done on the server level (server-based), between individual production and disaster recovery hot-spare server pairs, as well between two storage area network (SAN) solutions, one in production and the other at the disaster recovery site.

Solutions that employ data mirroring will also, typically, provide a method by which end users can remotely connect to the disaster recovery site and servers and work as if they were located in the production environment.

Since these types of solutions are delivering higher recovery point objectives and recovery time objectives, they are more complex than online backups and are considerably more expensive. But the major benefits of a data mirroring solution are:

- Data is automatically replicated offsite in "near real time," enabling higher recovery point objectives and;
- End users will be able to quickly access the data, features and functions needed to continue to operate or quickly return to operation after an outage has occurred, allowing higher recovery time objectives.

Data Protection: Tape Is Not Enough

One of the key issues in disaster recovery is protecting one of your most crucial assets: data. Due to increased regulations, financial firms are required to maintain a vast amount of data, however storing physical documents is not cost effective and does not ensure the safety of your information. Your data is too valuable for you 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 is an appropriate choice for day-to¬day restoration or long-term archiving.

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

Consider some of the uncertainties and questions that come with using tape:

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

Many firms are taking advantage of paperless document management solutions which allow you to capture, store, route and retrieve all your financial documents at your convenience to meet industry regulations and protect your business in the event of a disaster.

Hot Sites Versus Remote Access: 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, data and documents. The hot site also includes 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 continue working much as they did, pre-disaster, in the fund's production environment.

For a hot site to be most useful, your staff will need to be able to access it quickly. That implies that it would be located within reasonable proximity of your primary location. However, a hot site that is 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 willing or physically capable of traveling 50 to 100 miles to reach it, especially at a time of a natural disaster or unrest that leaves their homes or families vulnerable.

It is 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—in some cases on a first-come, first-served basis—with other hot site customers for the same facilities. Make sure you understand your rights and access privileges.

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

- **Lower cost.** You do not pay for office, real estate or telecommunications overhead because your employees access the remote disaster recovery site 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 IT resources that are dedicated to the firm and are housed and professionally managed at the remote site.
- **Greater convenience for employees.** An effective disaster recovery 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. Keep in mind, adaptability and flexibility are keys to any successful plan.

Regardless of which model best fits your firm's requirements, there are three important factors to include in your process: infrastructure, security, and testing and maintenance.

Infrastructure

The remote or hot site must have multiple levels of redundancy designed and built into every aspect of the facility aspect of the facility. Below is a quick checklist to help in your planning.

- **Network:**
  - ◊ Ensure your provider has redundant network equipment
  - ◊ Consider using multiple service providers

- **Power:**
  - ◊ There should be multiple sources, ideally sourced from different power grids
  - ◊ Are there backup power generators?

- How much fuel is onsite to run those generators? Where is the fuel stored?

- **Air conditioning.** Servers and other systems generate a significant amount of heat, making backup cooling systems a key component of a disaster recovery facility.

- **Security.** For data and telecommunications, your disaster recovery partner should deploy an uncompromisingly high level of security through technologies such as:
  - Virtual private networks (VPNs)
  - Virtual local area networks (LANs)
  - Firewalls, Intrusion Detection Systems and more

- **Redundant systems.** Whether it uses servers, routers or T1 lines, your remote or hot site provider should have "N+1" availability, a system configuration in which multiple components have at least one independent backup component to ensure system functionality continues in the event of a system failure.

- **Storage.** The best deployments leverage Redundant Array of Independent Disks (RAID) technologies to deliver striping of data across multiple disks for performance and mirroring/parity for improved protection and availability in the event of disk failure (RAID10 and RAID6 are best for data protection). Cloud providers may additionally retain multiple copies of your data in different data centers for ultimate protection.

- **Application software.** Ideally, your remote-site provider can accommodate multiple strategies, including redundancy, clustering, load balancing and warm standby (in which the application is loaded, but not running).

Security

From a facilities standpoint, you want your secondary disaster recovery site to have an even higher standard of physical security than your production environment or primary data center, as the disaster recovery site may experience a constant flow of people unaffiliated with your firm. Below is a list of some important site requirements:

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

Testing and Maintenance

The implementation of a disaster recovery plan is only the first step. A disaster recovery system is only useful if it is regularly and rigorously tested and maintained. When an outage strikes, you do not want to rely on an untested system only to find gaps, mistakes and failures that leave you without service.

Testing twice per year and ongoing maintenance allow you to find and fix gaps caused by technology changes or upgrades, and to train your employees on best practices so that they are fully prepared when the disaster recovery plan is executed.

The key to testing is to start off small and then build to a full, comprehensive test that includes an unannounced drill. 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 a background and training in disaster recovery solutions, as testing requires the shutdown of various systems and components to ensure appropriate failovers occur.

A checklist for essential plan testing guidelines includes:

- Provide detailed procedures to employees and closely follow them during a test.
- Verify the backup data and telephone trees.
- Test involving actual data.
- Change the scenario from test to test.

Conclusion

It would be easy to think that the smaller the hedge fund, the less risk there is; unfortunately, this is not true. In fact, smaller funds have just as much risk as larger funds. Therefore, it is essential that effective business continuity and disaster recovery plans be customized to the needs and environment of the firm, regardless of its size.

When dealing with business continuity or disaster recovery plans, there are many practices that should be incorporated and others that should not.

Some effective practices to follow:

- Determine an acceptable level of downtime during a disaster, based on business and application availability.
- Back up all essential documents and data offsite in an electronic format on at least a daily, if not in a near real-time, basis. Doing so ensures that if a disaster strikes, critical information is up to date.
- Establish the means to access essential information and applications in a remote manner. This could prove useful if an outage occurs by reducing downtime and enabling the business to remain running at nearly full capacity.
- Regularly test and update plans and systems to confirm that all personnel know their roles and that the technology is sufficient. This will help ensure that if the time comes, your systems fully operate and your employees know how to get the business up and running quickly.

Some of the ineffective methods to avoid:

- Relying solely on physical tapes for backup. If the originals of the backups are ever stolen, damaged or lost, all of your information is gone.
- Hosting your disaster recovery site at an employee's home. The many requirements—such as redundant power; heating, ventilating and air conditioning (HVAC) systems; fire suppression systems; and diesel generators—make running your site in a home impractical.
- Running your business dependent upon third-party Internet applications. If that application malfunctions or becomes unavailable, your business will suffer.

Sources:

[1] *Contingency Planning,* Strategic Research Corporation and Department of Trade and Industry 9DTI)/PricewaterhouseCoopers LLP, 2004.

[2] "Will Your Disaster Recovery Plan Work?" Alan Radding, *Storage Magazine*, 2005.

[3] "Best Practices for the Hedge Fund Industry Report of the Asset Managers' Committee to the President's Working Group on Financial

About Eze Castle Integration

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 600 alternative investment firms worldwide, including more than 80 firms with $1 billion or more in assets under management. Our Eze Private Cloud is the most widely used hedge fund cloud spanning three continents and supporting over 2,000 users and a petabyte of data. In addition to our cloud services, our solutions portfolio includes Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Geneva, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

The Eze Private Cloud is an enterprise-grade, private cloud infrastructure that provides hedge funds and investment firms a highly redundant, secure and available IT environment. The Eze Private Cloud is the backbone for Eze Managed Suite and Eze Managed Infrastructure.

To learn more about Eze Castle Integration, visit www.eci.com or contact us at 1-800-752-1382 or sales@eci.com.

About Pershing Prime Services

Pershing Prime Services delivers an unconflicted, comprehensive suite of global prime brokerage solutions, including extensive access to securities lending, dedicated client service, robust technology and reporting tools, worldwide execution and order management capabilities, a broad array of cash management products and the integrated platform of BNY Mellon. Pershing Prime Services is a service of Pershing LLC.

For more information, visit www.pershing.com or call 1-866-538-5046.