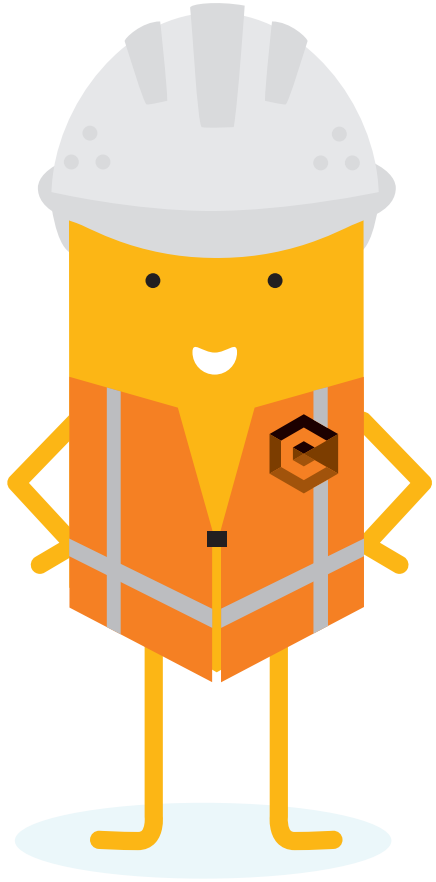
Disaster Recovery Options

BALANCING PROS AND CONS, OBJECTIVES AND COST

This ebook is written for both technology and non-technology executives who want to know their options and create a plan that appropriately balances protection and cost.



cosentry
We Operate. You Innovate.

DISASTERS ARE UNAVOIDABLE. YOU NEED A PLAN TO MITIGATE THE RISKS.

From the storm-of-the-century to the power line severed by a backhoe at a local construction site to human error, disasters come in many forms and levels of severity. However, even the most mundane can have a devastating effect on your business if it keeps you from engaging customers or causes you to lose data. You need a plan to mitigate the risks.

Of course, when creating a disaster recovery plan, you also need to determine the right balance of protection and costs. This e-book will help you decide which strategy is best suited to protect your company's data while avoiding nasty surprises when a disruptive event occurs.

Determine the right balance of **PROTECTION/ COSTS** when creating a disaster recovery plan.

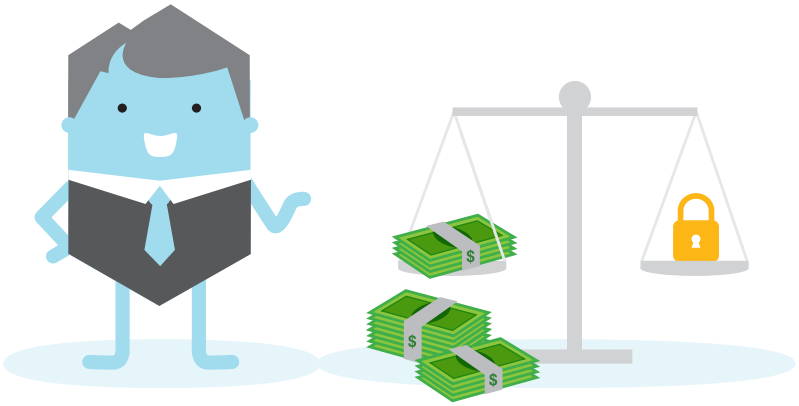
FACTORING COSTS INTO THE DISASTER RECOVERY EQUATION

Just as different businesses demand different approaches to IT, their approach to disaster recovery needs to be different, too. The types of disaster that can befall a business, from hardware failure to deliberate sabotage, are important to consider. However, two other metrics, RPO and RTO, need to be taken into account to avoid spending too much or too little on disaster recovery solutions – and ensure that you get what you paid for.

Recovery Point Objective (RPO)

RPO refers to the amount of time, e.g., 30 minutes, 24 hours, etc., for which is it tolerable to lose data should a disruptive event occur. RPO largely determines the frequency of data replication required in a disaster recovery plan. RPO often factors into decisions about tradeoffs between budget for your recovery plan and tolerable data loss.

Some businesses could survive losing as much as a few hours worth of data. Others would suffer irreparable damage if they lost just a few minutes. A short RPO, such as 15 minutes, indicates very little data loss is acceptable; a longer RPO, such as 24 hours, indicates less critical timeframes for preserving data.



SHORT RPO

(ie: 15 minutes)

very little data loss is acceptable

LONG RPO

(ie: 24 hours)

less critical timeframes for preserving data

Recovery Time Objective (RTO)

RTO refers to the window of time between a disruptive event and a return to operational status. In other words, the amount of time it takes for data to be recovered or restored. RTO largely determines the class of equipment and the means by which data is recovered.

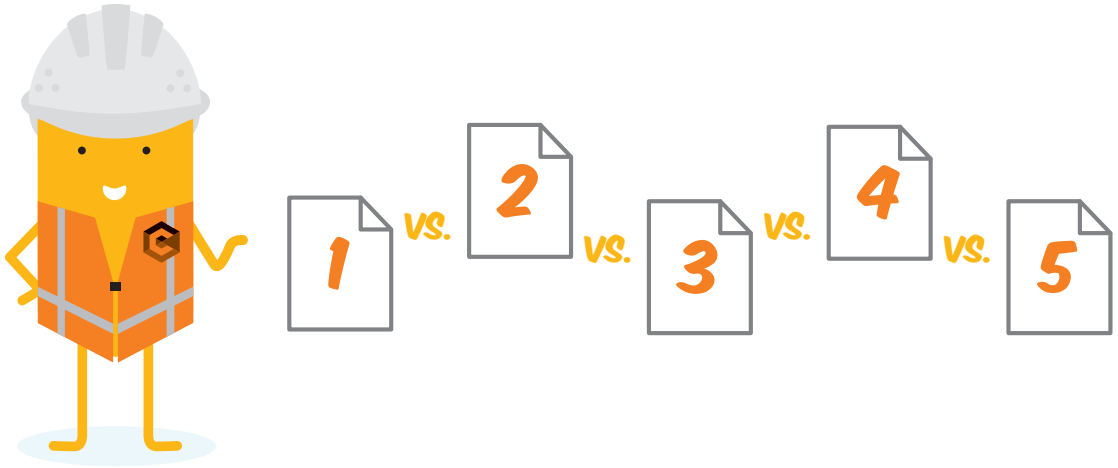
Highly seasonal businesses, especially in high-volume industries like retail, may decide that even an hour of downtime is more than they can afford. Other businesses may be able to keep things going without system access, at least for the afternoon, maybe longer.

Determine the Right Balance of RPO and RTO

Not only do businesses have different RPOs and RTOs, applications within a business will have different requirements as well. For instance, customer-facing applications usually demand a shorter RPO and a lower RTO because the loss of data and downtime can have a severe impact on the business. Internal or administrative applications that aren't as mission-critical may be able to withstand more downtime or a higher level of data loss.

Consideration of RPO and RTO for the business and for individual applications is vital when putting together a disaster recovery plan. Setting RTO too long or the RPO too high can put the organization at unacceptable levels of risk. Conversely, setting RPO and RTO at levels that are too aggressive leads to over-investment and ties up capital that could be spent in more productive ways.

RTO TOO LONG OR RPO TOO HIGH = UNACCEPTABLE LEVELS OF RISK AND/OR OVER-INVESTMENT



COMPARING OPTIONS

This ebook examines the many options available for disaster recovery and highlights the relative RPO and RTO tradeoffs against cost. In addition to providing you with a cost/benefit analysis, our goal is to provide you with the knowledge you need to ensure your plan successfully meets your organizational objectives.

Considerations:

- Many organizations use a combination of options to address various elements of their IT infrastructure and applications with different recovery requirements, which is perfectly acceptable. Depending upon the complexity of any given IT environment, managing the various options within the context of an overall disaster recovery plan or disruptive event can become challenging.
- Some managed service providers are starting to offer Disaster Recovery as a Service (DRaaS). Working with a provider can help you choose a solution that minimizes your costs while helping you reach your RTO and RPO goals. This ebook also will help equip you with the knowledge you need to successfully engage a DRaaS provider.

OPTIONS

1. Synchronous replication
2. Asynchronous replication
3. Cloud backup/ full system recovery
4. File backup
5. Local (tape/disk) backup

DEFINITIONS

Synchronous Replication

Synchronous replication is the process of copying data over a storage area network, local area network, or wide area network so there are multiple up-to-date copies of the data. Synchronous replication writes data to the primary and secondary sites at the same time so that the data remains current between sites. Synchronous replication is more expensive than other forms of replication, introduces latency that slows down the primary application and only works over distances less than 185 miles.

Asynchronous Replication

Asynchronous replication writes data to the primary storage array first and then, depending on the implementation approach, commits data to be replicated to memory or a disk-based journal. It then copies the data in real time or at scheduled intervals to replication targets. Unlike synchronous replication, asynchronous replication is designed to work over long distances. It does not require as much bandwidth as synchronous replication and can tolerate some degradation in connectivity.

Cloud backup/ full system recovery

Cloud backup, also known as online backup, is a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to an off-site server. In the enterprise, cloud backup services are primarily being used for archiving non-critical data only. Traditional backup, just as disk drives, is a better solution for critical data that requires a short recovery time objective (RTO.)

File backup

File backup is a method of offsite data storage in which files, folders, or the entire contents of a hard drive are regularly backed up on a remote server or computer with a network connection. This essentially is making a duplicate copy of your files and/or hard drive on a remote device.

Local (tape/disk) backup

Copying data to tape, CD or an external hard drive is quick and economical. This approach is commonly used by people who keep their data on the computer versus a server or the cloud. Once a week or so, the files should be backed up (at least the data files and perhaps the entire contents of the hard drive) to an alternative storage device that can be attached to a computer for backup and restore.

Definitions derived from Techtarget.com.

WORKING WITH A DISASTER RECOVERY PROVIDER CAN HELP YOU CHOOSE A SOLUTION THAT MINIMIZES YOUR COSTS WHILE HELPING YOU REACH YOUR RTO AND RPO GOALS.

OPTION 1

SYNCHRONOUS REPLICATION

Also known as Active/Active replication, real-time ("live") copies of your data are created and stored offsite. In the event of a disaster or system failure, key systems fail over to the backup site, keeping downtime and data loss to an absolute minimum.

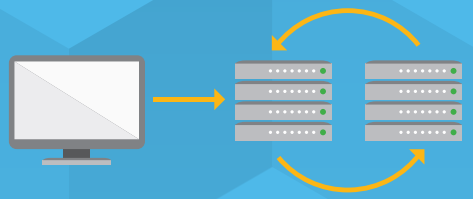
Your disaster recovery site should be geographically diverse from your main data center. Too many businesses located in the World Trade Center in New York discovered the problem with locating their data center in the building next door on 9/11.

PROS

- **Little to no downtime.** Recovery time is typically a function of boot time/order and any requisite DNS/routing changes. *(Best RTO of all solutions)*
- **Can be configured for automatic failover.** No loss of time due to manual switching.
- **Little to no data loss.** Data is always current as the backup site is always active. *(Best RPO of all solutions)*
- **Solutions often leverage checkpoints and journaling,** allowing the customer to failover to a specific point in time.
- **Allows for failback to production.**

CONS

- **Requires extra equipment and software.** (Highest cost of all solutions)
- **Requires reliable (and often high capacity) network connectivity** between locations.
- **Increased complexity.** Need to manage both sites and the connection between them.
- **Imposes a low latency requirement.** Often this is sub 10ms which may limit options for geographical diversity.



Typically, this high-availability approach couples real-time replication with redundancy in network and key infrastructure components. Synchronous replication is most often implemented at the storage level.

RPO: Best

RTO: Best

COST: Highest

IDEAL FOR: Organizations that absolutely must minimize downtime and data loss.

OPTION 2

ASYNCHRONOUS REPLICATION

Asynchronous replication, also known as Active/Passive replication, or a warm site, refers to a disaster recovery strategy where near-real-time copies of your data are created and stored offsite, either at a service provider's data center or at a second company location. Both synchronous and asynchronous replication strategies require a robust architecture that includes reliable connectivity between the primary and secondary sites. The desired RPO and the amount of data being modified will affect connectivity requirements.

PROS

- **Data is replicated continually.** However, unlike synchronous replication, activity at the primary site does not have to wait for the copy to complete to the disaster recovery site in order to continue.
- **Utilizing snapshots** allows you to replicate data on a scheduled basis at the time interval you specify.
- **No data restore is needed** – after a disruptive event, replica data becomes active. (RTO/RPO second only to synchronous option)
- **Can be configured for automatic failover.**
- **Allows for failback to production.**

CONS

- **Equipment costs are high to medium.**
- **Potential for some data loss.** Data is only current to last replication point.

Asynchronous replication can be implemented at the storage, hypervisor, operating system, and application level.

RPO: Minimal data loss

RTO: Fast

COST: Medium to high

IDEAL FOR: Organizations that can handle some data loss but still need to minimize downtime.

OPTION 3

CLOUD BACKUP/FULL SYSTEM RECOVERY

With this approach, your data is backed up via the Internet or a dedicated circuit to a secure location managed by your provider. Features can vary significantly from one vendor to another. For example, recovery time and complexity will increase if the vendor does not offer bare metal restore.

PROS

- **Easy to implement.** The vendor does the work for you.
- **Medium to low cost.** This approach provides a relatively short RTO and low RPO (although that varies by vendor) yet minimizes your investment in redundant systems.
- **Highly flexible.** Backup solutions can be tailored to recovery plans.
- **May be able to restore physical systems** to virtual machines.
- **Bare metal restore can be combined with backups** to shorten recovery time (included or optional feature of most backup software).
- **Backups can be automated**. With monitoring by a qualified provider, there is no need to worry about whether your data will be there in the event of a disaster.

CONS

- **Features vary by provider**. Plus, you should check to ensure the provider's backup software supports the specific applications you use.
- **Some providers may not support bare metal restore.**
- **Medium time to restore production.** This approach is slower than synchronous or asynchronous replication, yet can be considerably faster than restoring from a traditional cloud backup or local tape.
- **Restores are a manual process.**

If you are looking for a solution that balances cost and recovery time objectives, cloud backup with full system recovery may be the best choice.

RPO: Minimal data lost

RTO: Fast

COST: Low to medium

IDEAL FOR: Organizations that want to minimize downtime and data loss, but do not have the resources to manage disaster recovery sites.

OPTION 4

FILE BACKUP

There are a wide variety of companies offering this sort of service. Some cater to businesses while others cater to consumers. The most significant downsides to file backups are the time it takes to restore the backup and the limited full-system recovery options.

PROS

- **Low cost.** You only pay for what you use.
- **Good option for low volume of data** or relatively static data.
- **Web interface.** Generally easy to use, even for the non-technical user.
- **Uses existing Internet connection** for backup.
- **Typically, backup data is stored in geographically diverse locations.** No need to wonder if your data is sitting in a "hot zone".
- **Can be automated so the user doesn't need to "remember to back up the data".** This lends itself to better RPO than the local tape/disk backup.

CONS

- **The speed of the backup process is variable,** driven by the connection speed and user load at any given time.
- **Slower restore times.** When leveraging the Internet for data transport, bandwidth and latency constraints apply. Additionally, vendor offerings will differ in throughput capabilities.
- **Full system recovery, if possible at all, takes a long time.**
- **Users may not be notified of backup errors** or failure, and therefore unaware that backups are not completing successfully.
- **Restores are a manual process.**
- **Most services only back up data.** To recover, the business may need to reload and reconfigure applications first, adding time and complexity to the process of restoring operations.
- **Some services have limits on the amount of data** that can be stored and may charge for restores.
- **Not a good fit for organizations with large volumes of data** or that need a more aggressive RTO/RPO.

For some companies with a lower volume of data or data that is relatively static, file backup provides a viable option.

RPO: Good

RTO: Can be slow

COST: Low

IDEAL FOR: Organizations with low levels of relatively static data and can handle more downtime and data loss.

OPTION 5

LOCAL (TAPE/DISK) BACKUP

It all started with tape backup. However, as newer technologies have emerged, the old standby has been somewhat supplanted by more reliable options.

And we say "somewhat" supplanted because a survey by CIOinsight.com revealed that 48% of medium size businesses still use tape as a primary backup solution.[1] Although there are significant differences between tape and disk backup methodologies, we are listing them together because they both are carried out locally, generally without third party involvement.

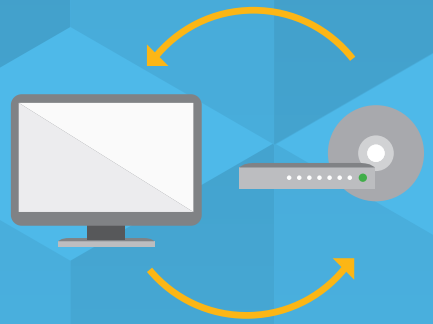
[1] Reisinger, Don, "Data Loss, Outages and Disaster Recovery." *CIO Insight.* Jan 3, 2013

PROS

- **Tape:** Low to low-middle cost.
- **Tape:** Cost effective for long-term storage/archiving.
- **Tape:** Well suited to be moved off site.
- **Disk:** Low-middle to middle cost.
- **Disk:** Can be cost effective for long-term storage/archiving when utilizing de-duplication technologies.
- **Disk:** Data protection capabilities can help eliminate data loss.

CONS

- **Tape:** High rate of media failure.
- **Tape:** Introduces security risks during tape handling.
- **Tape:** Retrieving backup from offsite location or vendor can delay restores.
- **Disk:** Susceptible to local site issues (fire, flood, power loss).
- **Disk:** Offsite capabilities typically require secondary hardware at a remote site or disk to tape export capabilities.
- **For both media, restores are a manual process;** full system recovery will take a long time.
- **The number of simultaneous restores is limited.**
- **Additional staffing costs may be required to manage backups.**



While tape may be a good alternative for some environments, testing is crucial given the potential for restore failure due to issues with the media.

RPO: Variable

RTO: Slow

COST: Low to medium

IDEAL FOR: Organizations with large amounts of data that can handle some data loss and potentially substantial downtime.

A SIMPLIFIED, COMPREHENSIVE SOLUTION

For many businesses, working with a Disaster Recover as a Service (DRaaS) provider makes sense. It allows them to set their RPO and RTO at acceptable levels, while minimizing costs. The money they save can then be invested in other business-building initiatives.

PROS

- Choose from a full menu of Disaster Recovery options according to your objectives
- Minimizes likelihood of overspending or under-protecting
- Single-vendor management of all DR plan components
- Benefit from experience and expertise of vendor
- Cost savings over a la carte/multiple vendor plan
- Expectations and requirements are usually outlined in a Service Level Agreement (SLA)
- Offsite vendors are less likely to be impacted by local/site events, and able to immediately put the DR plan in effect
- Can cover the entire production infrastructure including servers and storage
- Production environments are restored to the cloud, enabling a return to operations regardless of the physical state of your site

CONS

- Pricing models and services vary by vendor
- Vendor selection and on-going communication is critical to success of plan
- No "owned" offsite DR environment

Best of all, working with a DRaaS provider minimizes the time your IT department has to spend managing your backups or maintaining your replication site. They can now spend that time on more innovative IT pursuits that will help drive the business forward.

6-POINT CHECKLIST FOR EVALUATING A DRaaS VENDOR

DRaaS is a relatively new offering, and not all vendors offer the same set of services. Asking the right questions can help keep the unavoidable from becoming a real disaster. If you decide the DRaaS option is right for you, here are six criteria you should consider when evaluating the vendor's services.

#1 Protection for both virtual and physical equipment

Many companies today still rely on physical servers for certain applications. If that's the case in your organization, you need to be sure the applications the provider uses can protect both virtual and physical machines.

#2 Failover targets include both virtual and physical machines

If you do have physical servers that you are protecting often times these applications need to run on physical servers as well at the failover site. Not all DRaaS providers can support both.

#3 Defined testing parameters

Making sure everyone knows what to do should an event occur is an important element of any facilities disaster plan. Many organizations even test their plan by running practice drills. Likewise, the DRaaS provider should have a plan in place for testing your failover procedures so there are no unpleasant surprises in the event of an actual disaster.

#4 Transparent pricing related to declarations

When a disaster happens, and you have to run in the DRaaS provider's cloud, what additional costs are you going to incur? For example, during normal operations, you may rely on your own data backup procedures. However, during failover, you'll need to rely on the provider's systems and that will very likely incur additional costs.

#5 Security and compliance

Just as you need to ensure your data is secure and that you are compliant with regulations and industry standards like HIPAA and PCI, your failover site needs to be as well.

#6 Workgroup recovery options

Disasters affect people as well as equipment. If a disaster affects your physical location, your people may need a place to work. Some DRaaS providers can provide you with alternative workgroup options as well as vital equipment such as phone lines.

We got your back!

Cosentry manages 9 data centers across the Midwest, with Centers of Excellence for Data Center Services, IaaS (Infrastructure as a Service), DRaaS (Disaster Recovery as a Service), Compliance and Security.

cosentry
We Operate. You Innovate.

cosentry.com

QUESTIONS?

COMMENTS?

READY TO GET STARTED?

NOT SURE HOW TO START?

Call us at 1.844.COSENTRY (1.844.267.3687) or email info@cosentry.com