

Aligning disaster recovery and risk mitigation with business objectives.



TerenineSM Technology Solutions: December 2010

Disaster Recovery and Risk Mitigation: Considerations

As businesses become more and more reliant on technology systems, data storage, and electronic commerce, the impact of data loss on a company can be a game changer in today's economic environment. An effective disaster recovery environment enables your company to continue to work after catastrophic problems, such as computer viruses or natural disasters, strike the underpinnings of your business functions.

Do you know how well you are prepared?

Risk Mitigation

The level of risk mitigation in any environment can always be increased. No matter how well engineered, an environment can always be improved upon. There are no industry standard, predefined, risk mitigation levels. IT environments are too widely varied and specialized for this type of ranking system to be effective. The limit to watch for is when the cost of additional risk mitigation is higher than the loss of income resulting from an outage. One of the first things to determine, when considering implementing or changing a disaster recovery environment, is the cost-per-unit time of an outage (typically in dollars/hour) for each of the major parts of your IT infrastructure. This number will very quickly determine the level of risk mitigation that is cost effective.

Generalized levels of risk mitigation could be defined as types of disaster recovery options. These options will typically be: hot failover, warm failover, cold failover, hot backup, and cold backup. All failover options require roughly two times the infrastructure of a hot/cold backup option.

Hot failover is the most expensive option and will involve the least downtime. It requires data replication between at least two points. For the highest risk mitigation, those points will be significantly separated in terms of physical and geographical location. However, this separation can also cause issues. In order to have truly hot failover, synchronous replication is needed. In order to have synchronous replication, latency of no more than 60 ms between locations is

Disaster Recovery and Risk Mitigation: Considerations

required in most cases. Hot failover will typically require roughly twice the power consumption of cold failover or restore-based disaster recovery. Service interruption with this option will typically be measured in milliseconds (ms) or seconds. This option will require the most infrastructure and power.

The main distinguishing factor between hot and warm failover is that warm can use asynchronous replication and therefore is less expensive to implement across larger distances, as latency is less of a factor. Higher latency results in more service interruption and will typically be measured in seconds, which is acceptable for most environments. This option requires less power than hot failover, but it will still require roughly the same amount of infrastructure.

Cold failover is, for the most part, simply a warm failover setup where the secondary infrastructure is mostly powered off until needed. This gives it the advantage of less power consumption, but it also increases the amount of service interruption to minutes rather than seconds. Again, twice as much infrastructure will be needed, but much less power in comparison to warm and hot failover.

Backup-based disaster recovery will typically be the cheapest to implement, and will normally have the longest service interruption (measured in minutes, hours, or in some cases days). Because of how relatively inexpensive this option is, typically all of the failover options will incorporate this setup as well.

Hot versus cold backup is really only a distinguishing factor when database type applications are involved. In this case, a hot backup refers to setups where data can be backed up with no service interruption, while a cold backup would require service interruption for the duration of the backup job. Targets can be backed-up to tape or disk. Many will try to use a blanket-statement that disk is faster than tape; while normally true, this is not always the case (especially with the advent of the LTO5 tape standard).

Factors to Consider

There are many factors to consider when determining the appropriate disaster recovery environment. It will rarely be a single version of the aforementioned options, unless simple cold backup is chosen. Typical high-end IT infrastructures will incorporate at least three of the previously listed options, including at least one failover and both backup options. Rarely will warm and cold both be used, but all other combinations are likely to be seen.

1. **How much does an hour of downtime cost and what is the maximum acceptable time to recover?** Both of these factors will typically need to be posed multiple times for a given environment. The answer will usually be very different for a secondary Active Directory controller versus a mission critical MySQL server. When you know both of these numbers, it will be much easier to justify, or eliminate, options based on price. This is usually where failover versus traditional backup or both is decided.
2. **How much data and how many systems need to be protected?** This will be a large factor in the cost of the environment, regardless of which types are implemented. This will also be one of the major deciders of the types of backup media that are truly viable.
3. **What type of data?** This will determine the viable types of backup software and, in many cases, the acceptable forms of replication and the associated platforms.
4. **How long and how often?** There is a large price difference in monthly fulls, with one year retention and daily fulls with seven year retention. Often this is where the decision of disk versus tape versus both is decided. This is also where which type of each is determined.
5. **Where?** This is a consideration for both failover and backup. It is a substantial cost factor with failover, but it is typically to meet Best Practices, certification, or legal requirements when considered for backups. This also raises the need to consider encryption. It is a simple choice and should be dictated by the sensitivity of the data in question.

Disaster Recovery and Risk Mitigation: Considerations

As all of these are determined, legal requirements, certifications, and best practices should also be considered. If all of the above factors are considered with best practices in mind, then typically all legal and certification requirements are already going to be met. The possible exception is retention requirements which, depending on the industry, can range from 30 days to 99 years.

Typical Barriers to Implementation: Change, Cost, Time

As with any change in an IT infrastructure, there are always barriers to get through. The main blocking issues that we have seen, unfortunately, are typically the least relevant, once truly considered. The first that is typically found is a mentality of—if it isn't broken, then don't fix it. The really unfortunate thing with this is that the people that have to support the infrastructure, or recover it, rarely have this mentality. The harsh reality of IT is that if it isn't broken, it will be; even if the environment is picture perfect, meets all best practices, and is not abused or overtaxed. Eventually, a physical component will fail and a recovery of some kind will be necessary.

Usually along with aversion to change, cost will be a blocking factor. In some cases, the concern is legitimate. However, all too often, if the risks are truly weighed, the cost is completely justified. This is why it is so important to know the cost-per-hour of downtime. The individuals that take this stance, to block changes or implementation, are normally numbers-type people. Give them the numbers. We have seen companies balk at a cost of \$50,000 total to implement a backup solution for three years for a very large financial database (>1TB) that currently had no backups. When asked to estimate the value of the database, they stated approximately \$25,000,000. \$50,000 is a significant amount of money, but it is also only 0.2% of the value of what it protects. When this was pointed out, the opposition quickly faded.

One very legitimate barrier is time. Many simply do not have enough time to stop maintaining their environments to research, design, and build a disaster recovery



Disaster Recovery and Risk Mitigation: Considerations

environment. However, given how critical this issue is, if you don't have time—hire someone who does.

Conclusion

Disaster recovery must take into account how a business is run and the different elements required to keep the business going, as well as timeframes. These needs vary from business to business, and a good disaster recovery plan should be designed for the individual business's needs. This is our strength, aligning business goals with technology. Let the experts at Terenine help you evaluate your current environment and risks today.

What makes Terenine different?

Our Tier III Design Certified Data Center, [Terevault™](#), offers some of the highest levels of security, redundancy, disaster recovery, and maintainability in the nation. A certified Tier III Data Center must meet stringent infrastructure requirements and all aspects of the data center infrastructure must be concurrently maintainable. This means there are no single points of failure. Every piece of equipment, from heating and cooling to IT equipment, has a backup and can be removed for maintenance or replacement without impact on services or facilities. And, no annual data center shutdowns for routine maintenance are required.

**For more information, please contact the Terenine Sales Team at
866-379-3581.**

About Terenine Technology Solutions

Terenine Technology Solutions, based in Chattanooga, Tennessee, helps businesses find perfect alignment between business goals and technology innovation and service. Terenine offers a full array of technology solutions tailored to the customer's environment, including virtualization and cloud-based services, colocation, disaster recovery, backup and tiered storage, applications development, and professional services.

Terenine Technology Solutions, 1516 Riverside Drive, Chattanooga, TN 37406 www.terenine.com
Terenine is a service mark and Terevault is a trademark of Basenine, Inc., d/b/a Terenine Technology Solutions.