Data Center Series:

Business Resilience or Business Failure:

Pragmatic and Cost Effective Approaches to Disaster Recovery Planning

---

Provided by

NET(net), Inc.
+ 1 (616) 546-3100
www.netnetweb.com

Is Your Solution:

- Clear and Executable?
- Expensive and Ineffective?
- Federated across your multiple environments?
- Capable of meeting your Recovery Time and Recovery Point Objectives?

Read on, to learn more about what you can do in this situation.

IT Continuity

We have learned, among other things, we need to expect the unexpected. And while major weather events are the most egregious example of a disaster, we should be prepared for disruptions to the business on all fronts and all levels of severity. While it can be argued that Disaster Recovery and Business Continuity Planning is an expensive and tedious endeavor, it is clear that a well thought out plan that helps assure information technology continuity in the event of a serious disruption to the operation of the business, may well mean the difference between business success and business failure.

The primary objective of the IT continuity plan is to reestablish essential business technology operations should a disruption occur as a result of a disaster or other unplanned outage. The objective is to ensure that critical IT operations can resume normal processing within a reasonable period of time, and at a determined 'point in time' in the business. Therefore, the IT continuity plan should also:

- Identify potential weaknesses and implement a disaster prevention program;
- Minimize the duration of a serious disruption to business operations;
- Facilitate effective coordination of recovery tasks; and
- Reduce the complexity of the recovery effort.

IT continuity is also about high availability. It is about maintaining the IT operations of the business in the event of a serious failure or disruption affecting a data center location or a location affecting a business operation.

For instance, an objective for deploying distributed data centers is to provide redundancy, scalability and high availability. Redundancy is the first line of defense against any failure. Redundancy within a data center is just as important as redundancy between data centers, including application servers, databases, and communication and network linkages. Maintaining a comprehensive and rigorous backup and restore capability is central to establishing a business continuance strategy.

The Enterprise Approach

Enterprises often take a variety of approaches to disaster recovery planning, focused on the continuity of IT operations, and business continuity focused on the continuity of the business operation. A common approach is to maintain a primary and secondary data center, one or the other of which can be hosted in-house or with a third party data center hosting provider. However, this can be an expensive proposition for many organizations. Or a provider which specializes in IT recovery services may be employed, supplying "cold" servers that can be restored from the operating system to the applications to support the continuity of the IT operations within a specified recovery time objective. SunGard Availability Services is a common example in this space. An

approach common with most strategies is to at least store critical data offsite with a company that specializes in secure data storage such as Iron Mountain, using either the more traditional tape media or, increasingly more common—and often more affordable—online backups that are performed “disk to disk”.

The approach your organization takes with regards to disaster recovery, and specifically IT continuity, must be rooted in a comprehensive, achievable, up-to-date and tested disaster recovery plan. A plan that is lacking in a strategic and tactical vision for DRP, and is not comprehensive, achievable, up-to-date and tested, is typically the source of inefficient deployments of backup data centers, IT recovery services or backup strategy; needlessly throwing money at a DR solution without assessing the true risks and vulnerabilities to the business or deploying a solution that is either overkill or essentially wasted without having ever been tested.

For example, an enterprise subscribes to a monthly fee (often in the thousands of dollars) to have a provider set aside servers, storage, printers, networking and general infrastructure to allow the enterprise to recover all or a portion of their production environment in the event of a disaster, with a certain number tests and test hours allowed per year. The configuration for this environment (i.e. server, storage, networking specifications) is determined at the inception of the recovery services agreement. First, without a comprehensive test of restoring this IT environment, at least once per year, but ideally twice per year, the probability of expediently and efficiently—and successfully—restoring this environment to save the business is typically very low. All that money in disaster recovery services wasted and the business in peril.

Or, perhaps you test this environment from time to time, maybe annually, but the configuration is so out of date compared to the reality of your current production IT environment, that you have been paying for an environment that has been allocated on your behalf, largely for nothing; more wasted money.

BOTTOM LINE:

If your organization is going to go to the trouble of investing in the development of a disaster recovery plan to maintain the continuity of the IT operation, and spend the money to subscribe to a recovery service to restore your environment offsite, make the effort to plan the environment, plan the testing, conduct the testing and keep this environment up-to-date and relevant.

Another example is the deployment of a secondary data center for DR purposes, often the most practical choice of larger enterprises. On balance this option is typically less expensive than 3rd party recovery services for large data center footprints. However, the inefficiencies found in the primary data center, such as server sprawl, non-consolidated storage, obsolete applications, and under-utilized servers are often repeated in the secondary data center, wasting money and complicating a recovery effort in the event the primary data center needs to fail-over to the secondary data center. This issue is exacerbated if you are using a third-party co-location or managed services provider for this secondary data center because now you are likely paying an inflated expense to this provider for an inefficient DR environment.

BOTTOM LINE:

Keep the DR environment simple. Use VM technology to keep the server footprint small and the recovery effort less demanding during a real recovery effort. Apply good principles of server and storage consolidation, efficient use of existing resources and energy efficient devices to your DR data center to maximize the value of this environment.

Business Continuity

In addition to IT continuity services it is also common to accommodate business continuity. That is, allocate workspace for the workforce in the event the primary business location becomes unavailable for whatever reason for an extended period of time. This space can be allocated in another business office in the vicinity, a partner location, vacant office space or a third-party recovery services supplier that specializes in providing workspace, fully wired workstations, voice communications and other office automation in a business-like setting for a monthly subscription fee. As with the disaster recovery plan, the business continuity plan is only as good as the effort put behind it to properly plan, configure, test and execute on this environment. If you are paying a 3rd party services provider for this luxury and not testing this environment regularly and continually assessing the risk to need, this is more money wasted.

BOTTOM LINE:

Ensure your business continuity plan truly requires a third-party service to host your personnel. This option can be relatively expensive on a month to month basis over time for something that may never be used; perhaps the nature of the disaster precludes the personnel from even reaching the facility in a timely manner or it's determined that it would be much easier to just work from home. In fact, aside from an operation like a contact center or other operation that may benefit from housing everyone in one location, it is increasingly common, and arguably less expensive, to have personnel work from home in the event of a disaster or disruption affecting access to the facility, assuming they have access to the proper applications and networking from home; something that can be anticipated and planned for up front with a proper IT remote access plan.

The difference between business success and failure in the event of a disaster event that strikes your business and affects your IT operation just might be the due diligence you take in planning, preparing for and executing on your disaster recovery plan. Organizations that do this with discipline, efficiently and cost effectiveness, have a better chance of being rewarded with a successful recovery effort.

NET(net), Inc.
217 East 24th Street - Suite 010
Holland, Michigan 49423

© 2012 All Rights Reserved