How long can your agency operate without its data and applications? For an increasing number of
government organizations, the answer is not long.

Just about every operations process today relies on access to data and applications. Many are so IT
dependent that even a few hours of interruption can mean extensive production and services losses and a
damaged reputation.

In a recent IT disaster recovery survey sponsored by Symantec, respondents said that 56 percent of their
applications were mission critical on average, up from 36 percent in 2007.

If your organization has let disaster recovery (DR) slide, you’re taking a tremendous risk. Using an
ineffective, outdated strategy, not testing your existing plan or ignoring DR altogether means it’s time to
get serious about continuity of operations at your agency.

**Disaster Recovery Today**

There have been many changes in the disaster recovery field in the past five years. With the digitization
of more and more operations processes, increased use of the Internet and evolving legal regulations for
retaining information, storage volumes have skyrocketed.

Today it’s necessary to protect many more gigabytes of data than even just a few years ago. At the same
time, more and more agencies — large and small — have greatly increased their web presence and have
started offering more services online.

This increased dependence on digitized operations processes also means that many organizations now
have little or no recovery window. That’s why, for many agencies, the approach to disaster recovery used in
the 20th century, tape backup, is just too slow and labor intensive to work in the 21st century.

Luckily, disaster recovery technologies have caught up with disaster recovery requirements. Hard
disk reliability has improved tremendously while the cost of hard disk storage has come down to the
point where backing up to disk is a feasible, significantly faster, less resource-intensive alternative or
complement to tape backup.

Virtual tape library (VTL) technologies allow tape-formatted backup to highly reliable Redundant Array of
Independent Disks (RAID) hard disk configurations in a fraction of the time it takes to do so with a genuine
tape library. And it does this with fewer media errors and hardware problems.

Recovery is also much faster with disk-based VTL than with tape. And recovering individual files is simple
thanks to hard disk random search capabilities.

VTLs can also serve as a front-end to a genuine automated tape library. They take the backup burden off
of production systems and greatly reduce the need for a backup window.

Snapshot technologies, such as Volume Snapshot Service (VSS), originally introduced in Windows Server
2003, now allow regular incremental backups to disk several times a day, even while applications are
running. This technology can provide near-continuous data protection when used frequently throughout
the day.

Tape backups can then be run off the secondary disks using assembled incremental snapshots with no
need for a backup window as well. And with current snapshot techniques, incremental snapshots can be
run indefinitely without the need for full backups in between.

Long-distance data replication to servers and storage at a secondary site, once thought of as a viable
solution only for organizations with the biggest risks and most robust budgets, is now a feasible, cost-
effective alternative for many midsize agencies as well.
This is thanks to technologies such as deduplication. This technology eliminates backing up redundant data from, say, multimegabyte attachments e-mailed to 10 different staffers.

In addition, WAN acceleration and optimization technologies from manufacturers such as Riverbed, Blue Coat, Cisco and Radware slash bandwidth requirements. Thus they reduce WAN costs for replication.

Asynchronous replication, in which data is copied at preset intervals, is still much more common than synchronous replication. Also known as mirroring, synchronous replication is where new and changed data is written to both locations simultaneously.

**Virtualization for Recovery**

The technology that has perhaps made the most dramatic difference in disaster recovery is server virtualization. Server virtualization from VMware, Microsoft and Citrix abstracts the operating systems and applications from the physical hardware.

This technology allows you to pack several encapsulated virtual servers, each running its own operating system and applications, onto a single physical server, without worrying about conflicts. Virtual servers can be moved across physical boundaries from server to server at will, regardless of differences in hardware.

The effect of virtualization on replication costs and disaster recovery in general has been dramatic. Replication once required reproducing your entire production server configuration at another location, a cost-prohibitive scenario for most organizations.

Virtualization allows you to failover a physical server configuration to a virtual configuration using fewer, less-powerful physical servers at an alternate site. “You can populate your disaster recovery site with just a few older servers that you’ve retired from production and repurposed for DR,” says Jon Bock, group product marketing manager for VMware.

And unlike in the physical world where those failover servers must sit idle 99 percent of the time until they’re needed for failover, virtualization allows you to use those servers as production hardware for other applications at the same time. So besides lower bandwidth and storage costs, server hardware costs in a replication scenario are also reduced dramatically.

Virtualization also means that an entire virtual server, complete with operating systems, OS settings, patches, applications and data can be completely backed up by backing just a small number of files. So if a restore is required, there’s no longer any need for a laborious process of reinstalling and reconfiguring OSs.

There is no question that disaster recovery has become a bigger, more complex undertaking in the Internet age. Still the costs of high-level disaster recovery scenarios, including hardware, software, bandwidth and labor, have been reduced to the point where just about any organization can probably afford them.

**Building a DR Solution**

Does this increased importance placed on disaster recovery mean that you have to protect all your data using high-level technologies? Not if you want maximum cost efficiency.

The best way to protect your data is to understand what you need to protect and why. Then go about building the most effective and cost-efficient strategy for doing so.

This means undertaking a complete inventory of all your applications and data. Then define which systems are mission critical and which are merely important or not so important.

Determining which functions are mission critical is not that difficult. “If everything went down tomorrow, what pieces would you be unable to live without?” asks Mike Inkrott, senior production manager for Symantec’s Information Management Group.

While budgetary, operations-critical and forward-facing web servers immediately come to mind, other applications such as e-mail are increasingly falling into the mission-critical category. “Servers that have very high utilization are most likely to be mission critical,” Inkrott adds.

One development that has made this task more difficult is the increasing interdependency of applications.
Web servers may require application, database and other servers to function. And it’s necessary to identify all those servers that work together to support a mission-critical operations process.

“If I have a system with a web front-end and an underlying database, I can’t set the database recovery objective at four hours and the web at one hour,” says Rick Walsworth, director of product marketing at EMC’s Cross Platform Replication.

**Organizing Tiers**

Many organizations divide their applications and data into tiers. In this case, Tier 1 represents the processes that have to be up and running in minutes, while second and third tiers have less stringent requirements.

Each tier should be assigned a recovery time objective (RTO) and recovery point objective (RPO).

RTO refers to how quickly information and applications must be found, retrieved and accessed after a disaster. This generally helps to determine the type of storage you will use for backup and whether failover and replication are required. Anything under a few hours requires disk storage.

RPO refers to the point in time you need to recover to. In other words, how many minutes, hours or days of data and work can you tolerate losing completely after a disaster? If the answer is none, then you’re looking at a continuous data protection solution and/or replication.

In some cases, there’s another measurement to consider. Recovery granularity objective (RGO) refers to whether you need data recovered at the file, block or transaction level. VTL works for file-level recovery, while snapshots are often best for block level, and a continuous data protection scenario is often required for recovery at a transaction level.

**Types of Disasters**

The other thing to consider when crafting your plan is the types of disasters you need to be concerned about. You can’t possibly plan for everything, so you need to determine what type of disaster you’ll most likely need to recover from.

“In the south, you’re most likely talking about [natural disasters such as] tornadoes and hurricanes, so you probably want to think about replicating to a location outside the hurricane zone,” says Walsworth. “In the west, it’s earthquakes.”

Aside from major disasters, however, it’s important to also consider and plan for the most common day-to-day causes of outages, such as hardware failure, human error, software errors and malware (viruses, worms, etc.).

Unlike major disasters, these interruptions may require quick partial restores or the use of previous backups to return to a preinfected state. Malware is an important reason to continue to include tape backup as some part of your disaster recovery strategy.

The other thing to consider carefully is how to reduce the volume of data that needs to be replicated and/or backed up from each tier. With a sensible strategy that archives older, nonessential data and uses data reduction techniques such as deduplication, you can reduce your backup volumes, and thus costs, dramatically.

Finally, it’s time to devise a data protection strategy for each tier, taking into account your risks and recovery objectives. Each tier may or may not include some combination of backup technologies.

These can include snapshot technology, disk-based backups, virtual tape libraries and continuous data protection scenarios combining snapshots with tape backup, replication and other options (depending on your budget, risks and protection objectives). By tiering your protection intelligently, you achieve the ideal combination of maximum protection and cost efficiency.

It’s important to remember that while other media and strategies have replaced tape backup, offsite tape storage is still one of the most cost-efficient ways to protect yourself from disasters large and small.

It’s also important to update and test your disaster recovery strategies periodically as operations processes, applications and data evolve. Testing is made easier through server virtualization, which can allow you to simulate your disaster recovery scenario without having to take down significant numbers of servers.
Finally, continuity of operations strategies such as failover server clustering, RAID storage, redundant server components and load balancing should be considered as a prevention layer. They should be designed to reduce the number of incidents requiring disaster recovery implementation.

Like many other IT functions, disaster recovery has grown in complexity. At the same time, however, new options make automated, comprehensive disaster recovery strategies available for organizations on just about any budget.

Ten Steps for a Disaster Recovery Plan
1. Analyze your disaster recovery (DR) objectives.
2. Inventory your operations processes and their dependent applications and data.
3. Determine which processes are mission critical.
4. Evaluate the risks to data and applications, including probable disaster scenarios and partial loss scenarios from human error along with malware, power, hardware and software outages.
5. Create data protection tiers, each with its own recovery time objective (RTO), recovery point objective (RPO) and recovery granularity objective (RGO).
6. Create disaster recovery strategies for each tier that match your risk and protection objectives.
7. Implement your DR plan.
8. Test your DR plan periodically to ensure that it works and takes into account ongoing changes in operations processes, applications and data.
9. Update your DR plan periodically.
10. Employ continuity of operations technologies such as clustering, load balancing, Redundant Array of Independent Disks (RAID) and redundant components to minimize the need for disaster recovery.

How Virtualization Aids Continuity of Operations
Virtualization is quickly gaining appeal for its contribution to continuity of operations and disaster recovery initiatives. Because these initiatives typically carry a hefty price tag and level of complexity (not to mention extensive idle hardware), having virtualization assist in the process proves valuable in a number of ways, including:

- Allowing for less hardware at the recovery site;
- Facilitating easier failover and recovery;
- Snapshot technology can be used to capture a “point in time,” making for easier replication;
- Eliminating the need for one-to-one replication of hardware in a DR configuration;
- Allowing agencies to expand the scope of backup to all applications and data, not just those deemed mission critical.

CALL 800.808.4239 TO TALK TO A SPECIALIST TODAY.