

Valuable insights into IT disaster recovery management

In late October 2012, Hurricane Sandy made landfall in the Caribbean, mid-Atlantic, and northeastern United States with devastating impact, causing an [estimated \\$65.6 billion](#) in losses due to damage and business interruption. Here at Sungard Availability Services, we received 342 alerts and 117 disaster declarations due to Hurricane Sandy alone.

In the process of supporting our customers in their recoveries, we deployed nearly one-third of our staff, 5 mobile recovery units, 9 workgroup facilities, and 1,500 workgroup seats for our customers' employees. In addition, our [Carlstadt center also served as an impromptu community command center](#) for local law enforcement, medical, and first response teams. Here are some of the best practices and lessons learned that we felt would give you that all important head start when preparing for the next "Sandy."

We look at the IT recovery challenge as having 3 layers, all of which must be addressed in order to recover successfully.



IT Disaster Recovery is a 3-tiered challenge

In our business, we look at the IT recovery challenge as having 3 layers, all of which must be addressed in order to recover successfully:

1

Data Protection: If you don't have your data at an off-site, secure location, then you really have nothing at all. How you choose to get your data off-site – via tape, disk backup, storage replication, or server replication – will depend upon the mission-criticality of your particular applications and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each. However, simply having your data protected at a second location does not in and of itself make for a disaster recovery plan.

2

System Recovery: These constitute the platforms, servers, operating systems, backup software, backup hardware, hypervisors, networks, and storage that you will use to actually recover your applications. Your recovery environment should align with your production environment, and be compatible from all of the above perspectives. If your recovery environment has changed over time, then ideally you have performed adequate change management between your production and recovery environments so that when you attempt to recover your data, the two are in sync.

3

People, Processes, and Program:

- **People:** It should be obvious that it will be people — your staff — who perform the recoveries. Therefore, it is imperative that they have an operational place to work, with the right equipment, space, and communications to enable them to do their jobs. It is also important that they have the right expertise and focus to successfully recover your data and applications.
- **Processes:** These are the procedures and “runbooks” that document the steps of the recovery. Your recovery will only be as successful as your “last-known good” procedure, so if these are not updated or correctly maintained, then you run a significant risk of failing at recovering your applications and data.
- **Program:** This piece refers to the ongoing lifecycle and management of the DR program, and governs crucial activities like test planning and execution, post-test analyses, execution of change management, and active integration of best practices and lessons learned on an ongoing basis. We find that many of our customers do not have the wherewithal, time, resources, or budget to maintain a robust program conducive to an “always-ready” recovery posture.



With the aforementioned layers as our framework, we found that we had lessons learned and best practices to share at all three tiers of the recovery challenge.



Data protection lessons

We gained several insights into the data protection challenges faced by our customers, especially those who use tapes and trucks as their data protection strategy.

1

Transporting tapes to the Sungard AS facility for recovery purposes was a challenge compounded by the hurricane-induced flooding and road closures. As a result of their experience during Hurricane Sandy, many of our customers are **considering moving to disk-based backup or even real-time data mirroring and replication** as an alternative data protection strategy.

2

While tape is the least expensive medium for data backup, tape also requires the longest recovery times because the data is stored in a different format and requires rehydration. **If 24 to 48 hour recovery time objectives will not meet your business needs for applications that you backup to tape, consider moving to managed backup or vaulting services that leverage SAN replication technologies.**

3

Even if you elect to remain tape-based, you can still significantly shorten recovery times by taking advantage of best practices in parallel processing. For example, tape-based customers who have Sungard AS' Standby Operating System environment as a service have their O/S copies stored inside Sungard AS, which enables us to configure their recovery hardware and restore their operating systems while waiting for their tapes to arrive. This can significantly speed tape-based recovery.

System recovery lessons

Our customers run hybrid or heterogeneous environments — very few of them are all-physical or all-virtual. Their applications can have complex interdependencies, which mean that Tier 3 and Tier 4 applications must sometimes be recovered alongside mission-critical applications, because the latter often depend upon the former.

1

Change management is crucial. If the recovery environment is not totally compatible with the production environment, the recovery will fail. In a disaster situation, you do not want to have to negotiate last-minute changes to your contracted hot site because over time, you did not maintain production and recovery environment changes. This will only serve to delay your recovery. During Hurricane Sandy, almost one-third of our customers required significant changes to their recovery systems specifications, including having to obtain higher end servers, additional disk capacity, different tape technology, firewall configurations, LPARS for mainframe recovery, and LAN bridges.

2

Another common recovery pitfall was **failing to take into consideration all three layers of application tiers** — database, middleware, and web. We noticed situations wherein customers were unable to recover all three (some found a way to get the web tier back, but not the middleware or database tier, or vice versa). Failing to recover all three tiers leaves you stranded just as effectively as failing to move your data to a secondary site.

3

With regard to network connectivity, we advise that you **review your core network design and establish potential failover routes** to avoid network congestion around storm-affected areas.





The storm made it difficult for recovery teams to travel out of the area due to road and bridge closures, and many recovery personnel did not desire to travel out of their area to perform recoveries.

People, processes, and program lessons

The area where we observed the greatest number of lessons learned through the eyes of our customers was in the people, processes, and program tier.

1

People:

- **Telework and other alternative work strategies need to be revisited** in light of a regional disaster that saw power outages across large geographies.
- If your company **must comply with certain federal regulations mandating data privacy**, make sure you **contract for dedicated workspace** where your people and the data they are recovering can be kept sequestered from other companies' employees.
- **Don't under-contract** for workgroup space — if you will really need 200 seats to fulfill your recovery efforts, don't contract for only 50 seats.
- The storm made it difficult for recovery teams to travel out of the area due to road and bridge closures, and **many recovery personnel did not desire to travel out of their area to perform recoveries**. As a result, consider out-tasking your recovery to a qualified DR partner.
- **Focus on internal resource planning** and communicate in advance to employees regarding taking personal disaster measures, including how to get to the data center, personal family evacuation plans, etc. If you can, get recovery personnel to arrive at recovery sites before the storm hits, as closed-down roads, public transportation, and bridges eventually thwarted access to many locations.
- **Ask employees to fill personal vehicles with fuel prior to the storm's forecasted arrival!**



2

Processes:

- **Recovery runbooks must be kept up-to-date**, and procedures must be based upon current production configurations. With many customers failing to perform test management, recoveries were obstructed due to procedures that were based upon older versions of hypervisors, operating systems, or that did not reflect the latest software patches or upgrades.
- **Continuously update and audit your mass communications tools.** The best practice here is to pre-establish customer communications and communications with vital contacts specifically for disaster recovery purposes.
- **Identify and train on alternative communication tools**, so that if one form of communication is not accessible, a fallback is available. Even if you just had a good test, your recovery may still fail.

3

Program:

- **Even if you just had a good test, your recovery may still fail.** Planning for a test is on average a 12-week process; no hurricane provides that kind of advance notice. Don't rest on the laurels of your last test; maintain a constant state of readiness by ensuring post-test analyses are conducted and recommendations/best practices are integrated.
- **Perform rigorous change management.** As we've already noted, failing to flow production changes into the recovery environment is a recipe for disaster when it comes to recovery. Most, if not all, of our customers required a resource that was not a part of their contract, or a change from what was in their contract.
- **Consider "out-tasking" your Disaster Recovery program.** For many of our customers, disaster recovery is supported on a "best-efforts" basis. Many are experiencing budget shrinkage for DR-related programs, lack of staff availability for testing and change management, and a general lack of expertise and focus on disaster recovery. For these customers, out-tasking their DR program to a qualified provider like [Sungard AS could make the difference between recovery success and failure during crucial times \(like Hurricane Sandy\).](#) The benefits of partnering with Sungard AS for disaster recovery program expertise include improvements in recovery performance, increases in productivity and ability to focus on business value creation, cost savings, and a constant state of readiness for any eventuality.

Out-tasking your DR program to a qualified provider like Sungard AS could make the difference between recovery success and failure during crucial times (like Hurricane Sandy).



Valuable insights into IT disaster recovery management

Conclusion

Recovery is a multi-layer challenge, involving coordinating and optimizing your strategies along three fronts: data protection, systems recovery, and people, process, programs. The widespread power outages caused by Hurricane Sandy and similar events challenged our customers along all three of these dimensions. The data protection challenges they faced induced our customers to think more about acceptable recovery time objectives and potentially moving from tape-based backup towards real-time mirroring and replication technologies.

Given that so many of them required drastic changes to their recovery environments highlighted the importance of change management and keeping production and recovery in sync. Many customers realized that their recovery procedures were only as good as their last test, and that incomplete runbooks lengthened the time it took to recover their mission-critical applications, adversely impacting their business. This led them to evaluate Sungard AS as a potential partner in helping to create and manage the lifecycle of a long-term DR program that would free them to pursue higher-value workstreams.

Finally, Hurricane Sandy challenged the assumption that working from home was a viable business continuity strategy, and stressed the importance of securing enough private workspace to meet regulatory requirements and empower vital personnel to perform recoveries.

For more information please visit our website at:
www.sungardas.com/dr

Additional reading



[Epic Consequences — Expert Help in BC/DR](#)



[10 Things Your Team is Afraid to Tell You About Your DR Plan](#)

For more information

If you'd like to discuss any of the above best practices or lessons learned with us or to learn more about how we are partnering with companies just like yours to ensure the availability of mission-critical applications, please contact us at 1-888-817-0925.

About Sungard Availability Services

Sungard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software.

To learn more, visit www.sungardas.com
or call 1-888-270-3657

Trademark information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us

