STRATEGIES FOR MINIMIZING DOWNTIME BY MANAGING CHANGE

SUNGARD® Availability Services

MANAGING RECOVERY

Thought Leadership

WHITE PAPER

EXECUTIVE OVERVIEW

Most organizations believe they have adequate recovery plans in place. But the fact is, due to a lack of budget and time, change management gets neglected.

Not only that, the necessary investments in staff expertise can be overlooked, too. When these problems are in place, there are a number of consequences related to recovery. Testing becomes inadequate and more expensive. Recovery can be delayed or can fail. The business faces added downtime, lost revenue, and in the case of a failed recovery, an increased likelihood of closing its doors for good.

To effectively guard against these problems and ensure successful testing and recovery, you should outsource management of the full recovery lifecycle to an expert service provider. The service provider should assign a single point of contact to handle active maintenance of planning, procedures, data movement, testing, as well as the recovery itself and the reconnection of users. The service provider should deliver recovery at agreed-upon service levels at time of test and disaster. Finally, working with the service provider should create opportunities to strengthen and mature the production environment, as well.

A DISASTER RECOVERY "WAKE-UP CALL"

In today's business environments, network complexity, application divergence, and mobile device usage have contributed to a rise in man-made disasters. Failed equipment, network security breaches, and the lack of experienced professionals are increasing the number of outages and disasters businesses face.

Unlike more traditional disaster types, these "man-made" disasters often happen to you without warning, so disaster preparedness is critical to recovery success. If organizations are not conducting regular recovery testing, and not updating recovery plans regularly, the chances of getting applications and data back on line when needed are severely diminished.

To put it bluntly, the confidence an organization has in its recovery plan may be misplaced.

THE CAUSES OF INADEQUATE RECOVERY PLANNING

The root cause of inadequate recovery is a lack of budget and time necessary to create, configure, test and maintain disaster recovery procedures regularly and effectively. Specifically, it's a lack of resources required to properly maintain a recovery site, to retain sufficient on-staff recovery expertise, and to execute periodic testing. When these factors are underfunded or overlooked, the change management process starts to break down, with costly — and potentially dire — consequences.

Change management refers to the procedures in place to ensure the production environment and the recovery environment are in sync. If there is a configuration change in the production environment, it needs to be reflected in the recovery environment. And in most real-world organizations, changes to the production environment are happening constantly. In a typical environment with just 60 servers (see Fig. 1), a single change per month per system can result in more than 10,000 changes before each annual test. Keeping the recovery environment current with the production environment can become a monumental task for resource strapped IT organizations.

JUST **ONE** CHANGE PER MONTH PER SYSTEM

Production environment with 60 physical servers	**Recovery environment with 30 physical servers and 60 virtual machines**
60 operating systems +	30 operating systems +
60 security software agents +	30 security software agents +
60 management agents +	30 management agents +
60 infrastructure software modules +	30 infrastructure software modules +
60 application software modules	30 application software modules +
	60 operating systems +
	60 security software agents +
	60 management agents +
	60 infrastructure software modules +
	60 application software modules

CAN EQUAL **10,000+** CONFIGURATION CHANGES BEFORE EVERY ANNUAL TEST.

FIG. 1: The frequency and complexity of change means keeping your recovery plans and processes up-to-date is a huge task.

THE CONSEQUENCES OF INADEQUATE CHANGE MANAGEMENT

Delayed or failed recovery
During an actual recovery, inadequate change management can cause a disorganized and delayed recovery in a variety of ways. For instance, it might mean missing system and application updates must be applied during the recovery. There might be unknown bugs that have to be tracked down and patched. Changes to the hardware and infrastructure need to be accounted for. All of that has the potential to create added pressure on the recovery team at the time of disaster, added downtime for the business — and possibly a failed recovery.

Slower, more costly, or incomplete testing
Inadequate change management slows testing, too. Unexpected bugs in the recovery process and gaps in recovery procedures must be worked around on the fly. It might become clear too late that there is insufficient capacity at the recovery site to provide the performance required for the business. Critical component gaps might appear, like missing service capabilities, missing data, or an inability to reconnect users to the recovered applications. Consequently, the IT organization is left with a "best effort" — incomplete — result.

Making the testing process even more painful is the cost — as much as $100,000 per exercise, according to one Gartner study.

COMPLICATING FACTORS: STAFF EXPERTISE AND AVAILABILITY

If the lack of resources causing inadequate change management has also resulted in a lack of insufficient in-house recovery expertise, a number of recovery missteps can occur.

One of the most common problems is an inadequate understanding of the interdependencies among the systems and applications being recovered. This can result in a failure to properly sequence the restart of applications. There may be insufficient expertise readily available to recover complex database systems, or even to rebuild and restart backup servers.

And, trained or not, during a real disaster IT staff may be unable or unwilling to travel.

THE BOTTOM LINE

For an organization relying on the availability of its applications and data, a disorganized or delayed recovery adds unplanned downtime, which can lead to lost customers and lost business.

OUT-TASKING YOUR RECOVERY LIFECYCLE

There is a better way.

The recovery lifecycle (See Fig. 2) covers everything from planning and infrastructure through managing recovery when disaster strikes. And for most IT organizations, a better strategy for managing the recovery lifecycle is to hand over the reins to an expert service provider. The service provider is then responsible for each phase, including:

- Actively managing and maintaining the recovery infrastructure, whether it's cloud, dedicated physical, or a hybrid of the two.
- Data movement to and from the recovery site using technologies selected to meet the recovery requirements of your specific applications
- Fully managed restart of simple and complex applications
- Full responsibility for meeting the recovery time and recovery point objectives you've agreed upon
- Finally, the ability to reconnect users seamlessly, whether remotely, with mobile recovery units, or with specialized workforce recovery facilities

When you partner with the right service provider, you gain assured application recovery, fully managed, and under contract to meet agreed-upon recovery time and recovery point objectives. You can be assured that recovery experts will be available during real disasters, and focus 100% on your recovery. Along with the lowered business risk, the resulting operational efficiency means less administrative burden on the IT organization and the ability to focus on strategic business initiatives.

But how do you find the "right" service provider to manage your recovery lifecycle? There are a few things to look for.

FIG. 2: The recovery lifecycle is the essential foundation for all SunGard Recovery Services.

PROCEDURE DEVELOPMENT
- Develop recovery procedures

TEST PLAN
- Schedule equipment
- Define configuration for testing

TEST SETUP
- Setup and configure infrastructure and hardware

OS STARTUP
- Build backup environment
- Restore OS
- Configure network

RESTORE
- Restore databases
- Restore data
- Restore applications

DATA SYNCH
- Synchronize databases

MAINTAIN
- Update/Correct procedures
- Change management
- Maintain procedures and configurations

IDENTIFYING THE BEST SERVICE PROVIDER FOR YOUR ORGANIZATION

Applications-focused recovery
Finding the "right" service provider for an organization means selecting one that takes that applications-focused approach to recovery. That means the service provider is going beyond infrastructure to help identify which data and applications support critical business processes. This is important because by focusing on the requirements of specific applications, the selection of recovery technologies and processes are tied directly to the needs of the business. As a result, under- or over-provisioning infrastructure is eliminated and recovery at time of test or disaster becomes more organized.

Applications-focused recovery also defines sufficient applications performance for recovery, rather than viewing application recovery as a binary "on." Additionally, this approach allows for the recovery of complex applications with point-in-time recovery of data if necessary.

Value-added management of recovery testing
The key to effective recovery is effective testing. Expert recovery testing often reveals problems in production environments—and it can even help strengthen the primary applications environment, protection systems, and change management at production site.

Partnering your recovery needs with a service provider automatically reduces the cost and burden of testing by eliminating the need to travel to and from the recovery site. But the service provider should also work with the organization to further limit recovery testing and exercise costs. This starts with effective change management to maintain alignment between recovery processes and the production environment. The right service provider will also assist the IT organization with planning test scope, including identifying what to test and how often — critical questions to answer to avoid over-spending as well as under-spending

Full responsibility for the complete recovery lifecycle
Most importantly, the service provider should be selected based on its ability to provide complete management of the recovery lifecycle. That means a full suite of recovery services that manage the lifecycle end-to-end, from securely delivered custom recovery plans to service customized for each specific applications environment. Find out if the service provider has the expertise in place to manage the recovery of complex, interdependent applications and services, which present a critical recovery challenge.

WORKING WITH A SERVICE PROVIDER TO MANAGE RECOVERY

Working with the right service provider will begin with plan scope and implementation. Recovery procedure runbooks should then be custom-developed to support the specific applications environment and the agreed-upon service levels.

But on a day-to-day basis, one point of contact should be assigned to the organization and should work as an extension of the IT staff. This liaison will coordinate the active maintenance and management of the recovery processes, and will know an organization's recovery lifecycle and procedures better than the organization itself.

THE ADDED BENEFITS OF OUT-TASKING RECOVERY

External recovery expertise can help strengthen a primary applications environment, too. That's because testing recovery often uncovers gaps in a production operation, which, when filled, improve production processing and can even lower costs. The supplied recovery runbooks can also be used for partial recovery of applications in a production environment. And the ready expertise can lead to a streamlining or redesign of protection systems, which can result in increased efficiency and cost savings.

CONCLUSION

Most organizations lack three fundamental components essential to managing recovery from a disaster: continually updated recovery processes, staff availability for test and recovery, and on-staff recovery expertise. Finding the right service provider with the experience necessary to deliver effective recovery management cover that gap.

ADDITIONAL READING

Five Simple Steps for Transforming Your Application Backup with Online Recovery Services

Data Security and IT Strategy within a Holistic Approach to Meaningful Use

About SunGard Availability Services

SunGard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software. With approximately five million square feet of datacenter and operations space, SunGard Availability Services helps customers improve the resilience of their mission critical systems by designing, implementing and managing cost-effective solutions using people, process and technology to address enterprise IT availability needs. Through direct sales and channel partners, we help organizations ensure their people and customers have uninterrupted access to the information systems they need in order to do business.
To learn more, visit www.sungardas.com or call 1-888-270-3657.