THE C-SUITE GUIDE TO MAXIMIZING AVAILABILITY

Best-laid IT Recovery Plans

We operate in an "always-on" economy. Your employees, suppliers and customers expect that systems and applications will be available 24/7/365. This means your business infrastructure must be highly available and that your business applications is paramount. Unfortunately, your business is constantly facing unpredictable forces that are often out of your control.

FEMA indicates that almost 40% of businesses never reopen following a natural disaster.[1]

To address such issues, many companies design highly available production environments as well as develop extensive IT recovery management plans only to see them fall apart when the unexpected happens.

A global benchmark study found that 73 percent of companies are unprepared for disaster recovery. Additionally, the study finds 78 percent those companies experienced outages of critical applications, leading to losses from a few thousand dollars to over $5 million. Many things can occur to prevent a successful recovery, even for those situations that have been identified in a business continuity plan, and prepared for through previous recovery tests.

To fulfill the goal of IT availability needed to compete in today's "always on, always available" world and ensure your recovery efforts are successful, it's a good idea to ask your staff five critical questions. Based on the answer to these questions, you will have a better idea if your IT recovery plans have you covered or need revising. This paper discusses those questions and provides strategic recommendations to take into account before the next outage affects you.

What's at stake?

In the event of an unexpected disruption, can your critical applications be restored fast enough to prevent damage to your business? With the memory of Hurricane Sandy fresh in our minds, this issue should create a greater sense of urgency. The Federal Emergency Management Administration (FEMA) notes that almost 40% of businesses never reopen following a disaster.

You might feel confident that you are protected by a well thought-out recovery management plan (also known as a disaster

SUNGARD AVAILABILITY SERVICES®

[1] http://drbenchmark.org/global-benchmark-study-reveals-73-of-companies-are-unprepared-for-disaster-recovery/

[2] http://www.fema.gov/protecting-your-businesses

A Business Impact Analysis (BIA) helps you understand the potential consequences of a disruption on your business. The financial and operation impact results from the BIA will help your company better prioritize your recovery efforts

recovery (DR) plan). Unfortunately, many organizations find they are caught flat-footed when a disruption occurs.

For a recovery plan to work, it must be frequently tested and updated, with your staff continuously evaluating changes in applications and business requirements. What has been performed in your production environment should be reflected in your recovery environment. This is no small task. You must account for perpetual OS changes, software updates, patches and user rights/configurations that go on in a given month within your organization. If these hanges are not reflected in your recovery environment, you might not have the right information or the correct user rights to access the application or data. Even worse, the data may no longer be aligned with the applications configuration, causing you to lose the data.

If you do not think this is an issue in your organization, consider the consequences if you are wrong. While many DR-related blunders are not made public, there have been enough catastrophic failures recently reported across the media that highlight how DR plans can fail if they are not frequently updated and fully tested. In one case, a major supplier of financial information suffered damage due to failures that extended into its (presumably) redundant systems.

In another, someone at a major studio ran the "RM*" delete command on Linux and UNIX workstations and nearly lost an entire year's work in 20 seconds. As tends to happen in data disasters, the local backup system had also been failing for a month without being noticed, so the film was gone. Luckily, one of the animators had the entire library of animations backed up on her home computer...but we will save the topic of data loss prevention for another time.

QUESTION #1: Have you done a Business Impact Analysis (BIA)?

A key element to any DR effort is carrying out a Business Impact Analysis (BIA). This is the only way to understand the potential consequences of a disruption on the business. Once you have this information, your company can then prioritize its recovery efforts.

The BIA should identify the operational and financial impacts that would result from a disruption. This helps establish the costs to the business when an application or service is not available.

On the surface, developing a BIA is straight forward. When evaluating an application, check

[3] http://www.nytimes.com/2015/04/18/business/dealbook/bloomberg-terminals-outage.html?_r=0
[4] http://mentalfloss.com/uk/entertainment/27204/how-one-line-of-text-nearly-killed-toy-story-2

Gartner estimates that the average company loses over $300,000 per hour of network downtime.

to be sure all aspects of its worth to the company are taken into account. Start with the obvious. What would be the revenue loss per hour if an application was not available?

But also consider other business factors. What would be the regulatory and legal impact? Would the organization be at risk for not meeting a contractual obligation? Would there be compliance issues, such as those that can occur if, for example, required data is not recovered in time to meet the demands of an auditor, regulator or subpoena? The financial impact when records are unavailable or destroyed can be significant.

Consider the long-term business impact of even a brief disruption. With today's competitive market-place, a loyal customer finding an ecommerce web site unavailable might switch to a competitor. That could result in the loss of that customer's business forever.

Are there additional costs that would be incurred due to the unavailability of an application or service? For example, if a payroll system is down, what is the cost to manually print checks and pay employees using a third party? If a production line is disrupted, would there be penalties or late fees for not meeting delivery dates? Or would you need to contract with a third party to temporarily take over a business operation until restoration was complete?

Using this approach, you can then gauge which applications and services are most important and thus need to be recovered in the shortest timeframe. Essentially, a BIA will help you define the required levels of availability, Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for your critical applications and non-critical applications.

Question #2: Have you tiered applications and do you understand application interdependencies?

If you are satisfied your team has done a thorough BIA, the next step is to be sure they use that information to prioritize recovery efforts. Specifically, you need to find out if they have categorized the DR requirements for all applications.

The reason this is important is because of the financial impact when critical applications are down. Gartner estimates that the average company loses over $300,000 per hour of network downtime.

Using the information from the BIA, your staff should establish RTOs/RPOs for each tier of application to help determine recovery priorities and DR cost justifications. A common way this is done is to assign tiers in the following manner:

Many of today's business-critical applications present availability and recoverability challenges due to interdependencies with secondary applications.

- **Tier 1:** < 4 hours RTO
- **Tier 2:** 4 – 12 hours RTO
- **Tier 3:** 12 – 24 hours RTO
- **Tier 4:** 24+ hours RTO

This will help your company determine which methods to use to restore an application and how to capture and move data to a secondary site. For example, with Tier 4 applications you might not need a hot standby ready, relying instead on bringing a new system up to handle an outage. You might also have more flexibility in what data is restored, relying on the physical shipment of yesterday's backup tapes between sites. For Tier 1 applications, you would need a complete backup environment at the ready in a secondary site. And you would need to use replication technology that ensures faster data recovery, which is important for applications with low RPOs.

Having tiered your applications, you need to ask your staff if they have taken application interdependencies into account. The reason? Many of today's business-critical applications present availability and recoverability challenges due to interdependencies with secondary applications. That means restoring a critical application might require that lower tier applications are also restored in line.

For example, many of today's ecommerce applications are essentially three-tier web applications. They often include a database, middleware, and a web server layer. These different applications typically run on systems with vastly different availability characteristics. They also make use of multiple storage platforms, multiple compute platforms, multiple operating systems and a mix of physical and virtual environments.

If something goes wrong and you need to recover the application at your recovery site, you will have to restore all three layers for the primary ecommerce application to work properly. If you can only get the web layer back in less than four hours without restoring the other two layers, your site would not be able to take customer orders and you would lose revenue.

Using the information determined in a BIA, the RTO/RPO requirements can be leveraged to develop service level agreements (SLAs) for each application. Having those SLAs, you can determine which technologies and approaches to use to restore each application.

Question #3: Have you tested all applications?

Once the restoration plan is defined and put into place, you must test your processes to ensure they work. This means doing a complete test where applications and data are restored. While this sounds

The lack of change management with recovery procedures is one of the most significant root causes in recovery failures.

like a given, in practice it is not done enough.

There are numerous examples where unjustified faith in a DR plan left an organization hanging after a disruption. Take the case of a Civil District Court in New Orleans a few years ago. What seemed like a routine recovery of the county's conveyance and mortgage records database after a server crash exposed a major problem.

Without conducting a full restoration test, what went undiscovered was that despite an indication that an upgrade to its backup software had been successful, the installation actually failed. And for nearly a year, new records that were thought to be backed up were not, all while old copies were purged every 30 days. The end result: Not only were all changes and new entries that occurred after the most recent backup lost, but so too were all records dating back to the 1980s.

The only way to avoid problems like this is to conduct full tests of your DR plans. And even when a plan works successfully, do not rest on your laurels. In today's dynamic business environments, there are frequent changes to production systems (including routine maintenance and software upgrades) that can lead to problems and impede recovery. So test and retest.

QUESTION #4: Have you taken change management into account?

As noted above, today's dynamic production environments (which are subject to numerous and constant patches, upgrades, and changes) can quickly get out-of-sync with backup environments, causing potential recovery problems.

Compounding the problem is the fact that many business applications typically run in highly virtualized and cloud environments. This means changes in the past that would have been documented and planned, can now be made quickly without taking the change's impact on recoverability into account.

Such changes mean that recovery scripts that worked in the past might not work now. What is needed is a complete accounting for any changes. Unfortunately, many companies neglect this point in their DR planning. And as a result, the lack of change management with recovery procedures is one of the most significant root causes in recovery failures.

Ask your staff how they address this issue. Do they maintain runbooks and proper change management practices to ensure backup environments reflect these changes?

Technology solutions alone do not guarantee recovery success. People and processes are critical.

QUESTION #5: Have you taken people and processes into account?

Most companies focus on the technological aspects of DR. But technology solutions alone do not guarantee recovery success. People and processes are critical.

Ask your staff how they ensure the right people know how to execute the right processes at the right time to restore business operations after a disruption.

Do you have well-defined and frequently tested processes? Does your staff have a test schedule and are these tests frequent? Are there runbooks in place to guide a restoration process?

Are people with the required expertise in place to carry out the steps in a runbook? How are those people notified when an outage happens? What happens when they are not available (as was the case in many companies after Hurricane Sandy when roads were closed and flooded and there was no gas)?

As part of the people and processes examination, you must address one additional point. Many companies do not take into account that over time, as business priorities change, so do restoration priorities. An application that was considered critical two years ago might not have the same recovery urgency today. So build re-categorization into your DR processes. If the RTO of an application shifts from Tier 1 to Tier 3 over time, why keep it at Tier 1 and misallocate resources when the staff could be working on more important chores?

Conclusion

To keep one step ahead of current and future threats to system and data availability, assess your risks to quantify the business impact of downtime for each mission-critical application. Once this is determined, decide what the acceptable (if any) downtime is for each application and set recovery time thresholds.

Next, develop a strategic approach to recovery and select solutions that will help restore systems in the desired recovery time frames. Part of this work should include examining the people and processes issues related to your recovery management plan.

Asking the questions highlighted in this paper can help you determine if your organization is better prepared. If, by answering these five questions, you determine that your organization is not properly prepared, you will now have the visibility and the tools to minimize the impact of an outage, and provide true availability for your business.

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

GLOBAL HEADQUARTERS
680 EAST SWEDESFORD ROAD
WAYNE, PA 19087
484 582 2000
www.sungardas.com

EMEA HEAD OFFICE
UNIT B HEATHROW CORPORATE PARK
HOUNSLOW, MIDDLESEX TW4 6ER
+44 (0) 800 143 413
www.sungardas.co.uk

BELGIUM
+32 (0)2 513 3618
www.sungardas.be

FRANCE
+33 (0)1 64 80 61 61
www.sungardas.fr

INDIA
(+91)20 673 10 400
www.sungardas.in

IRELAND
+353 (0)1 467 3650
www.sungardas.ie

LUXEMBOURG
+352 357305-1
www.sungardas.lu

SWEDEN
+46 (0)8 666 32 00
www.sungardas.se

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

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

SUNGARD AVAILABILITY SERVICES®

IT FOR BUSINESS THAT NEVER STOPS