



## Key Considerations for **Disaster Recovery Planning**

**Learn how to achieve uninterrupted access—no matter what**

It used to be that disaster recovery fell solely within the domain of technical specialists and engineers. That's no longer true; these days, it's imperative to share this important responsibility among both executive and IT management. By considering these “key considerations” and the answers to them, your company is taking the first steps toward protecting its technical and business environments and improving its Information Availability strategy—the ability to keep people and information connected throughout the enterprise—no matter what.

Implementing Information Availability strategies can help you to deliver the secure data, systems, networks, and support required to keep employees, suppliers and customers connected and help your business stay in business—and get back up quickly when you have an outage!

1

**Is the continuity of your organization a top-level priority or something sitting at the end of a long list of initiatives that need to be handled?**



In the past, there were only a few select types of companies that were required to have formal plans in place for disaster recovery and business continuity, notably those in the financial services, healthcare and government sectors.

Now, industry regulations, compliance issues and financial audits place an extra burden on almost all types and sizes of businesses. They require you to maintain formal processes for emergency management and internal disasters. They insist that you safeguard confidential or sensitive information. And they demand that you're able to restore essential services and resume business as usual while dealing effectively with your own disaster scenario.

That's why executive sponsorship of your Information Availability strategy is a must. Starting at the top, the board of directors must be made aware of existing risks and proposed solutions and encouraged to authorize the funding for implementation. Additionally, your entire management team needs to provide unconditional support across the enterprise, making it a top priority for everyone so that your systems and workflows are truly recoverable within the recovery timeframe you've set. And this support should be communicated to all departments at all levels, to foster staff knowledge and obtain their buy-in. When top management establishes and shares the continuity strategy, it then becomes a sound, viable plan that lets you recover IT operations and continue with business as usual despite interruptions.

# 2

## How complete is your plan?



An IT-focused disaster recovery plan is only a partial solution. You must have a comprehensive program that addresses business as well as IT recovery: information, systems, people and processes, as well the complex interdependencies among them. It's the only way to make certain that your company can stay focused on its strategic mission.

Such a plan involves obtaining a deeper understanding of your organization, its IT and business environments, and the internal and external pressures that drive them. It means researching and collecting data on both departmental and technology resources and requirements, as well as how they affect each other. With this type of holistic overview in place, you can determine where you stand, what needs to be improved and how you will plan to maintain operations in the future. With this level of preparation, your organization will benefit from quicker, more efficient, more cost-effective resumption on all fronts following an interruption.

# 3

## How do you determine a realistic budget for an Information Availability strategy?



That's a tough, but legitimate question. And it requires a top-down view of the entire enterprise to make sure that smart, cost-effective technology decisions are made throughout.

One of the first things to do is analyze your risk and evaluate the total cost of ownership (TCO) of the risk mitigation approaches available. You'll need to factor in direct costs for things like hardware, software, staffing and utilities, as well as indirect costs, such as floor space, power protection, physical and information security, and management overhead, among others.

Then you must determine your availability requirements per application and system as well as the strategies for recovery—ranging from limited or single-service options to full-scale, managed solutions from a service provider you can absolutely trust.

With this information in hand, your company can derive a true TCO to help determine which approach to recovery best meets your financial considerations as well as your availability needs and recovery time objectives (RTO).

# 4

## Where do employees go and what do they do in a disaster?



There's no doubt that recovering data and systems efficiently is important. But it's equally imperative to get essential work functions up and running without delay. As an employer, you need to address the logistics of planning for the people and place aspects of recovery with a thorough business continuity plan.

One of the first things to do is to identify alternate locations where employees can go in the event a primary work location is unavailable. These end-user locations must be equipped with technology and business resources—ranging from computers and phones to desks and chairs—that allow for recovering systems and resuming business as usual. And, for some businesses, healthcare providers, call centers or financial services organizations, managers and other staff must also have manual processes in place to keep critical processes running efficiently until the recovery is complete.

This planning must include other components, such as an incident notification and escalation strategy. It also needs to address the physical safety and psychological well-being of employees. Finally, it must be well communicated throughout the organization so that everyone knows how to respond in a disaster situation.

# 5

## When was the last time you ran through a scheduled test of all aspects of your disaster recovery program?



Even the best-laid plans have snags. Consequently, your organization needs to prepare and execute a testing schedule to make sure all aspects of your program come off at time of disaster. The smart move is to seek guidance from a third-party services provider with an established track record in your industry. In that way, you'll benefit from someone who can help you execute successful tests that incorporate real-world experiences with expertise in the multiple platforms and applications you use. You'll also be able to choose the testing option—hotsite, mobile data center, remote site, remote testing or turnkey solution—to fit your staffing requirements and budget.

Working with experts also helps ensure a thorough test. They can offer assistance with the pretest preparation, making sure you have the right data backed up, not versions created for testing, and the right procedures defined. They will help you load tapes and other media to bring up your systems and applications. And, finally, they will work alongside you and your IT staff, running through testing scenarios that demonstrate your ability to recover, and pinpoint areas for improvement.

# 6

## Where are your internal IT resources focused—and at what cost?



Certainly, your organization needs to handle routine IT activities, such as security, network operations, software support and storage. But it also needs to focus on more strategic initiatives that are needed to run your business, today and in the future, as well as provide financial benefits.

You can rely on in-house staff but they're often immersed in daily workday responsibilities. By enlisting the help of SunGard, you can receive support to help you work toward achieving longer-term goals. SunGard can also supplement your strengths—with extra staff, specialized expertise, advanced technologies or a ready-made technical infrastructure. Partnering with SunGard also allows you to scale up or down as needed while maintaining control over the IT operation. Our approach is to let you offload as much, or as little, responsibility as you see fit. Just as important, this alternative helps you realize lower operating costs, reduce capital investment and avoid hidden expenses, especially when compared to an in-house alternative.

# 7

## Have you thought about how much you rely on e-mail?



Organizations of all types and sizes are finding that e-mail is becoming the communications method of choice, necessary for supporting day-to-day operations. Especially in today's regulatory-intensive environment, e-mail security, archiving and availability are issues that can't be ignored. Making electronic communications safe but readily accessible—without focusing too many internal system or personnel resources on it—should be a top priority.

To be effective in this endeavor, it's important to analyze your entire e-mail management process, with the aim of developing an end-to-end solution that addresses the creation, distribution and archiving of e-communications. First, it needs to provide for a way to keep your messaging system up and running, with full e-mail capabilities, during an outage that affects your IT infrastructure or place of work. Next, it should include best-in-class protection that guards your systems against intrusions such as viruses and spam. Finally, this solution should focus on compliance with the varied directives that regulate these communications.

# 8

## How safe is “safe” when it comes to your data and systems?



Security is a top IT priority these days. That's partly due to the increasing number of threats to data and systems that come from outside and within. For many organizations, there are the added security measures arising from compliance directives, such as Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA. They require that you have plans that demonstrate your ability to recover and access data and systems, so protecting these assets and reducing risk become all the more critical.

It's a daunting task, however, considering that new ways to breach your security perimeter materialize almost daily. A viable solution is to enlist the support of certified security professionals from SunGard. With experienced consultants in your corner, you can better assess your defenses and identify areas where IT and business resources are exposed to risk—both the physical and cyber varieties. They'll help you analyze your current environment, processes and planning efforts, holding them up against healthcare industry practices and standards. The outcome will be an effective, enterprise-wide security program that reduces your vulnerabilities and improves security and safety throughout.



## Where are the missing links in your value chain?



Service Level Agreements (SLAs) are commonplace today—and these contracts go both ways. You may be bound by an SLA to your customers and may also have such agreements at work in your vendor relationships. The environment that is required for these services is more complex than it used to be, currently requiring a computer system, a telephone call routing capability, a recovery site, a network and desktops—and it must all be operational in a lot less than the traditional 48 hours. Without a solid plan in place, there is no way that these types of SLAs can be met.

However, industry research shows that many firms would not be able to provide their contracted levels of service and support following a disaster. Organizations often do not have a business continuity strategy and plan that adequately addresses the requirements outlined in these agreements. Nor do they adequately test the ability of suppliers, such as telecommunications services or hosting providers, to hold up their end of the bargain.

An effective continuity plan should address your entire value chain: the implicit and explicit requirements your organization places on third parties, as well as the commitments you have made to others. You must consider the penalties and other costs—including those imposed by regulators and auditors—that would be associated if you fell down on your end.

# 10

## What have you done to address your data?



Data is usually the passion—and responsibility—of the IT department, not senior executives. But it's something that all management needs to consider. The availability of information, not to mention the continuity of your business, depends on good, usable data. And chances are, your data isn't as sound as it needs to be to support an actual recovery.

Today's applications are far more complex than ever before, not to mention they are interrelated with other applications and processes as well as running on multiple platforms.

### What's an organization to do?

Consider these hard-and-fast guidelines:

- Identify critical data to reduce backup and restore time and resources;
- Set standards of ownership for data used by multiple applications;
- Establish an enterprise-wide records retention program covering both electronic and paper files;
- Synchronize restored data across applications and platforms;
- Conduct integrated application recovery tests to prove true recoverability; and
- Integrate data security measures into your continuity plans.

**SUNGARD**® Keeping People  
Availability Services and Information  
Connected.™

680 East Swedesford Road  
Wayne, PA 19087

800-468-7483  
[www.availability.sungard.com](http://www.availability.sungard.com)

**recall**™

180 Technology Parkway  
Norcross, GA 30092

1-888-RECALL6  
[www.recall.com](http://www.recall.com)