

Product Brief

SunGard Continuity Management Solution: More than Just Software – An Intelligent Framework

Date: January 2011 **Author:** Jeff Hine, Consulting Analyst, and Bob Laliberte, Sr. Analyst

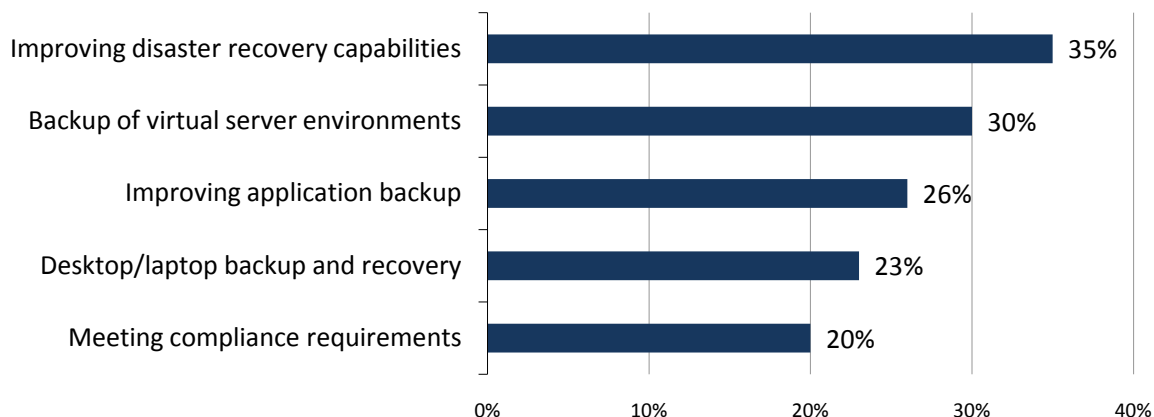
Abstract: Deep in the halls of many IT organizations lives a worrier: a professional paid to assume the worst, plan for disasters, and contemplate the unthinkable. They are the Disaster Recovery Planner. They may prefer “contingency” or “business continuity” as part of their identity, but their role is clear: document what needs to happen to keep the business running and teach the rest of us our roles. [SunGard](#) Continuity Management Solution (CMS) is a suite of software tools and best practices that help automate and maintain a functional and auditable DR plan.

Overview

Disaster recovery means different things to different people. For some, it’s as simple as mirroring two disks or having the office admin grab a backup tape and throw it in their trunk at the end of the day. To the mega-corporation in a regulated industry, it means industrial strength server and application clustering, remote storage, multiple sites, and mountains of binders. Even the term “disaster recovery” often sparks debate: shouldn’t we be talking about “business continuity” and trying to figure out how to come back from an outage or, even better, never go down in the first place? The concept encompasses more than just technology to include emergency response, communications, workforce continuity, and reliance on external service providers. Regardless of your definition or situation, there are few concepts in technology that become more contentious than how to spend money on and plan for an event you hope will never happen. At the end of the day, how much time and money organizations allocate to plan creation and testing varies widely and is a direct measure of both the level of confidence in technology and the potential impact of an outage.

Figure 1. Top 5 Areas of Data Protection Investment for 2010

In which areas of data protection do you believe your organization is likely to make the most significant investments in 2010? (Percent of respondents, N=510, multiple responses accepted)

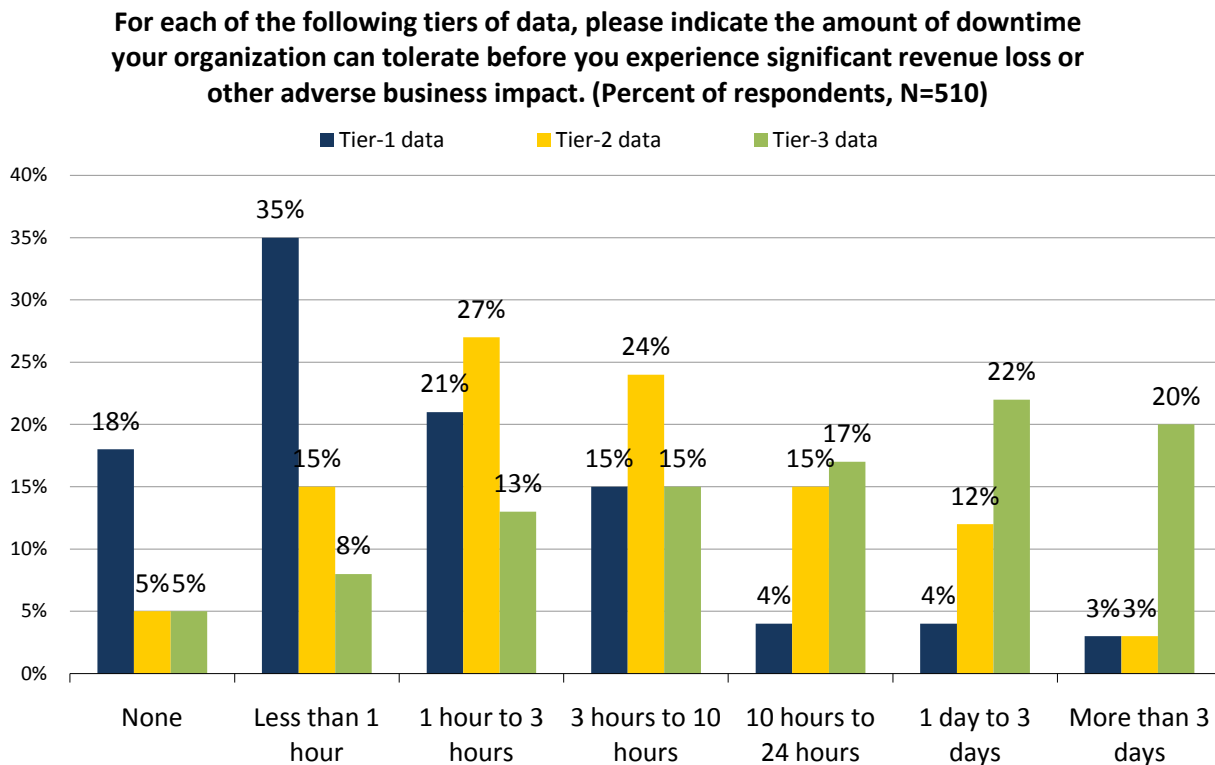


Source: Enterprise Strategy Group, 2010.

In a recent ESG study on data protection trends,¹ 43% of respondents cited a lack of a disaster recovery plan or process as a challenge with their overall data protection strategy. It is not surprising, then, that more than one-third (35%) of respondents expect their organizations to spend money specifically to improve disaster recovery capabilities in 2010; in fact, it is the most commonly selected area of data protection investment (see Figure 1).

Another element to consider is the fact that all data is not created equal. Organizations spend a tremendous amount of time analyzing both the profile of the business data they are trying to protect as well as the interdependencies that exist between systems. Of the survey respondents, 74% of organizations claimed that they could tolerate no more than three hours of downtime related to tier-1 data and applications (see Figure 2).

Figure 2. Downtime Tolerance According to Business Value of Data



Source: Enterprise Strategy Group, 2010.

So how do companies plan and protect themselves against an outage caused by system failures or loss of access to their data or facilities? And how do they accumulate, synthesize, and document all of the information, including dependencies by tier of data and criticality of business process?

One thing we do know is that when companies get serious about these issues, they commit people resources, not just technology; technology alone rarely solves business problems. Companies that are serious have full-time planners paying attention to this problem. In addition to their own time, passion, and creativity, these planners rely on software tools to turn what can be a time-intensive, detail-dependent, risk-laden process into an organized, cross-functional effort.

¹ Source: ESG Research Report, [2010 Data Protection Trends](#), April 2010.

SunGard Continuity Management Solution

The SunGard Continuity Management Solution (CMS) is much more than just software. It provides an intelligent framework and a fundamental way of thinking about how to approach the continuity planning process. You could consider CMS a DR consulting practice in a box, representing the accumulated knowledge of more than 20 years of best practices in DR and contingency planning. In a business environment demanding continuous access and a competitive landscape where losing access to data or losing access to customer service means lost sales, business leaders cannot just believe that technology will save them. The age-old adage is more relevant today than ever: if we fail to plan, then we plan to fail. The following are some of the critical aspects of plan development that CMS addresses:

Start with a solid foundation. LDRPS (Living Disaster Recovery Planning System) is the cornerstone of CMS, automating the maintenance of and creation of the contingency plan. LDRPS leverages Navigators which consist of automated interfaces that bring a planner through a step-by-step process of creating elements of their plan. Using Navigators, planners can facilitate productive conversations with end-users and business constituents to build plans which cover all critical elements; templates and best practices take the guesswork out of creating a plan that covers all the bases.

Centralized intelligence and dependency mapping. Once populated through a combination of questionnaire-driven interviews, custom entry, and imports from a variety of supported data sources, LDRPS is the core of a powerful relational database from which planners can manage and report on all aspects of business continuity. One of the more useful elements of LDRPS is the ability to map dependencies. Mapping technology dependencies has always been a challenge in IT. Whether planning for a recovery, migrating data between critical systems, or moving IT assets from one data center to another, understanding what application is associated with what server and what storage is not only a critical element for a successful move event, it is a major element of risk reduction. Imagine having a system outage and simply not knowing what applications were running on the failed server or what downstream systems or process might be impacted. Now take this mapping one step further: LDRPS provides not only a dependency view of underlying technology, but also a macro view of entire business processes. The organization can make links between technology and associated business and organizational processes, allowing leaders to set SLAs and response plans accordingly.

Feature-rich assessment modules. One of the most powerful aspects of SunGard's CMS is the investment it has made in its "Assessment" modules. One fate that can befall even the most useful and sophisticated software tool is that of becoming shelf-ware. This happens for a variety of reasons, but more often than not is due to a combination of time and skill-set constraints that prevent the user from following through on the noble goals they had when the software was first purchased. Assessment modules prevent this and help derive true business value from the solution.

The assessment modules serve as wizards, guidebooks, and best practice templates for conducting analysis and evaluating major financial and operational vulnerabilities and dependencies planners need to consider when constructing and maintaining a DR plan. In addition to BIA Professional, SunGard has developed three additional assessment modules to date.

Vendor Assessment – Recent ESG research on the cyber security supply chain showed that only 31% of organizations always audit the security procedures of an external vendor or service provider.² In an interconnected business environment, we'd expect this number to increase over time, and understanding an external providers' recovery readiness should certainly top the list of concerns. The Vendor Assessment module guides planners with questionnaires and best practices to conduct and audit of external vendor providers in the areas of risk, crisis management procedures, and overall continuity plans. Built-in intelligence then allows planners to rank and rate external vendors, giving them an overall score. This is an area that many plans miss due to a focus on internal risk, not taking into account the plans of external entities their business relies upon.

² Source: ESG Research Report, [Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure](#), November 2010.



Workforce Assessment – All the greatest technology in the world and platinum level failover will not matter if critical employees are not in a position to do their work. Whether it's remote connectivity giving them the ability to be productive at home or recognizing that a regional disaster may make an entire segment of the workforce unavailable, no plan is viable unless it considers how people will remain engaged and productive through a contingency event. The Workforce Assessment module guides planners through the process of understanding how to keep their employees productive, who the critical employees are, and how to communicate with them. With the advent of technologies such as VDI allowing users to work anytime, anywhere, it will be critical for planners to understand the work habits and dependencies of an evolving workforce.

Risk Assessment – Mitigating risk is what contingency planning is all about. The Risk Assessment module, based on sites/locations, allows planners to provide executives and the organization as a whole with a macro view of the overall risk to the business in a multi-dimensional fashion, taking into account natural disasters, human risk (e.g., the disgruntled employee), or geographic risks and model the potential impacts and responses. The information synthesized here can not only help executives make the right decisions around investments to mitigate those risks, but also serve as a foundation for regulatory compliance.

Analysis

LDRPS has a 20-year heritage of being the market leading solution for disaster recovery planning. SunGard has taken this core and expanded on it through the addition of advanced features and functionality. One disadvantage that SunGard has is that the most prevalent alternative solutions are essentially free. Companies have already invested in general productivity tools such as Excel, Access, and Visio which can be leveraged to create the necessary elements of a DR plan. What these solutions do not provide, however, is any level of automation in keeping a plan up to date or built-in intelligence to make the end product better.

In a look at the market as a whole, SunGard CMS shines brightly by combining software technology with best practices to:

Make it easy. If it's hard, people don't bother. Do you really want to tell regulators and investors that DR planning was too hard and time consuming with Word, Excel, and Access, so you just couldn't maintain the plan? DR planning isn't easy, but CMS does make the planning easier and far less time-consuming. Leveraging Navigators to build the plan, leveraging Assessments to populate the plan with the right data, and running reports from a relational database offers better visibility and will make a thank-less job into one that makes you look like a superstar. Everyone likes easy and everyone wants to be a superstar.

Demystify the black art and leverage wisdom. Beyond just software, the questionnaires and Navigators represent the accumulated wisdom of 20 years of best practices and input from professional disaster recovery planners. One interesting thing to note about CMS is that training is free. That means people are keeping their skills up to date continuously. In addition to training, there is a robust and active user group community supporting this software. This tribal knowledge feeds a development team and makes the software a reflection of this collective wisdom. This means that planners of all skill levels benefit from this knowledge and the business itself benefits from the fact that the software makes the planner smarter about how they create and maintain the plan.

Create fans. As part of writing this piece, ESG spoke to M&T Bank, an LDRPS user since 1997. A top-20 regional banking firm, M&T operates two data centers in the northeast and supports thousands of users accessing terabytes of storage.

M&T takes recovery management seriously. LDRPS is at the heart of the creation and testing of its DR and emergency response plans. Aside from all of the normal things you would expect to hear from a 13-year client, M&T finds particular value in how the software has evolved over the years and how it has allowed and enabled its continuity and recovery plans to evolve. One of those key new elements it is taking advantage of is the dependency mapping. M&T has been building out extensive process maps of all the banks' core functions for two years. In fact, the software itself has helped guide M&T to truly understand exactly what a dependency within the business process means and how to model appropriate SLAs and link infrastructure and process directly to the business.



It was clear from ESG's conversation with M&T that this software has not just satisfied users, but inspired fans: people who take these skills with them from company to company and even go so far as choosing jobs based on whether or not the company uses LDRPS for its planning.

The Bigger Truth

I'll take a better planner over better technology any day. No technology expenditure, no geographic distance, and no CDP appliance or big iron will bring your business back from disaster if you don't know what application runs on which system, who owns the system, how to communicate with them, or if the system supports a critical business process. And by "know," I mean standing in front of the CIO three minutes after a disaster is declared and telling him or her that everything is under control. That's the reason you have a plan.

But we have to remember that it's not really just about the planner—it's all about mitigating business risk. Leveraging SunGard's CMS does, in fact, make the planner more effective and more productive. But most importantly, it makes the business more secure and reduces risk. And this is the whole point. Companies don't invest in this technology because it makes the planner's life easier. They invest in it because what makes the planner better also makes the business safer.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.