

# White Paper

---

## **Redefining BC/DR Planning for Midsize Organizations**

*By Jason Buffington, Senior Analyst; and Monya Keane, Research Analyst*

**November 2013**

---

This ESG White Paper was commissioned by Sungard Availability Services and is distributed under license from ESG.

## Contents

The Importance of Midsize Business BC/DR Planning.....	3
Calamities Happen at All Scales: The Danger of Unpreparedness .....	3
Midsize Organizations Need BC/DR Even More than Enterprises Do .....	4
Commodity-industry-related ‘Soft Costs’ Also Figure into the Picture .....	4
Understanding the Business Continuity Planning Process .....	5
Much More Than Technology—BC Planning Encompasses People and Processes.....	5
Don’t Think Bits; Think Dollars.....	5
Backup Isn’t BC/DR, and the Skills Aren’t Synonymous .....	6
The Best Part of BC/DR Is the Preparation, not the Recovery .....	7
Sungard AS Recovery Services .....	8
Application Availability .....	8
How Sungard AS Is Redefining BC/DR for Midsize Organizations .....	9
The Bigger Truth .....	10

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.

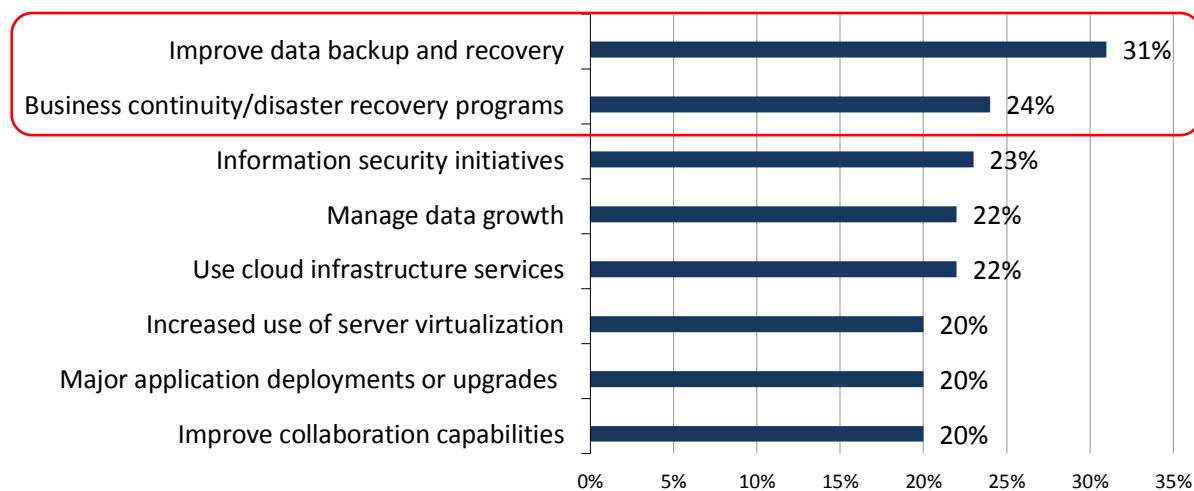
## The Importance of Midsize Business BC/DR Planning

In the information era, nearly every organization considers data protection a priority. For some, it's a *really* big concern. For others, it *really* should be.

Midsize organizations (businesses with between 100 and 999 employees) are even more likely than their larger enterprise counterparts to identify data protection as a top IT priority over the next 12 months, according to research by ESG. In fact, data protection—specifically, improved data backup and recovery processes and business continuity/disaster recovery programs—accounted for the top-two overall most important IT priorities mentioned by midsize organizations (see Figure 1) in response to ESG's survey.<sup>1</sup>

Figure 1. Top Eight IT Spending Priorities for 2013 Among Midsize Organizations

Which of the following would you consider to be your organization's most important IT priorities over the next 12 months? (Percent of respondents, ten responses accepted)



Source: Enterprise Strategy Group, 2013.

Even looking beyond the midmarket-specific IT priority filter, respondents across the broader midmarket-plus-enterprise landscape named improving data backup and recovery (27%) and business continuity/disaster recovery programs (20%) as two of their most important IT priorities overall for 2013.<sup>2</sup>

### Calamities Happen at All Scales: The Danger of Unpreparedness

So, backup and recovery as well as BC/DR continue to be hot trends, especially for midsize companies. But a bit of caution should accompany this emphasis. Namely, BC/DR conversations should not always be held in the context of prepping for a "most dreaded and dire catastrophe," i.e., major tornadoes, hurricanes, floods, or blizzards capable of disrupting entire regions.

In reality, organizations need to think about mitigating/combatting a wide range of potential disasters—for example, a localized power outage affecting just one building, or a cooling problem that has taken down a single aisle of servers at the secondary location's site.

Calamities happen at all kinds of scale. However, the *practices* and the *methods* of business continuity planning still apply, regardless of how broad the disaster's scale is or how big or small the affected IT components are. Remediation methods remain applicable; it's really just a matter of size.

<sup>1</sup> Source: ESG Research Report, [2013 IT Spending Intentions Survey](#), January 2013.

<sup>2</sup> Source: Ibid.

And, no matter what assumptions one might make about how expensive it would be to deploy mitigating technologies/availability solutions or how time-consuming it would be to develop a business continuity plan, remember this: The cost of downtime *inordinately* exceeds the cost of BC/DR preparedness efforts.<sup>3</sup>

## Midsize Organizations Need BC/DR Even More than Enterprises Do

Historically, the IT industry perceived BC/DR preparedness as an activity less viable for small and midsize organizations than for enterprises operating sophisticated infrastructures according to mandates from shareholders or industry regulations. Perceptions about a lack of affordable, usable, right-sized technologies also persisted within midsize organizations.

If something goes bad in a *big* enterprise, typically, IT professionals are present on staff who have years of focused experience in maintaining/restoring IT operations. They can put on their proverbial superhero capes and “save the day.” But even in those large enterprises with their presumably greater IT technology resources and operational IT experts on hand, the expertise to plan efficiently for and then execute rapidly on the recovery of whole environments can be a rarity.

In contrast, IT pros in midsize companies have to be flawless multi-taskers. They are often so busy that they can barely manage to keep the lights on. Midsize organizations don’t have an IT “Clark Kent” onsite who does nothing other than ensure business continuity. They just have Clark’s empty phone booth. In other words, when a midsize organization needs disaster recovery help, it has to call for help.

Thus, when a disaster-related outage happens, not only are these organizations down operationally (losing productivity and profitability), but they also have to pay (often exorbitantly) for third parties to come in and help them repair themselves. And although those costs can vary dramatically, the reality is that while the company is unable to generate income or maintain customer satisfaction, they are paying consultants and outside experts—essentially hemorrhaging superfluous cash just so that they can get running again—without any additional value to show from those extra expenditures.

It *is* counterintuitive to accept that midsize organizations need a strong BC/DR strategy as much as or more than enterprises do. After all, big enterprises deal with more revenue and run more elaborate and widespread business operations. Why shouldn’t it be comparatively more important for them to be available? Here’s the key, though: Big companies often have the most advanced high-availability systems on the market embedded into their core architectures, and they have experienced IT heroes (although BC/DR specialists far less so) on staff. Midsize organizations typically have none of that, but they have just as much dependency on their data, servers, and IT services.

## Commodity-industry-related ‘Soft Costs’ Also Figure into the Picture

From a soft-cost perspective, another challenge arises. A lot of midsize organizations produce and sell “commodity” offerings—they are raw materials manufacturers, for example. Or perhaps they offer services such as lawn-sprinkler installation, sign-making, pest exterminating, etc. The problem with commodity offerings is that when the company selling them is down for any length of time, potential buyers seek the equivalent product elsewhere in quick fashion. Whether you are an IT pro supporting a midsize tax-prep firm, a local movie theater chain, a midsize construction company, an online ticket reseller, etc., it doesn’t matter. If customers can’t get the commodity they need from you because your company’s systems are down, they’ll waste little time going to your competition.

---

<sup>3</sup> As one proof point, a Google outage in August 2013 reportedly caused by an IT infrastructure problem lasted just five minutes but cost \$500,000. <http://www.hngn.com/articles/10372/20130819/google-outage lasted-5-minutes-global-traffic-down-by-40-percent-google-loss-totals-500-000.htm>.

## Understanding the Business Continuity Planning Process

One major and often-observed failing related to BC planning centers on assuming that the admin in charge of backup operations is going to be the best person to devise and deliver the company-wide BC/DR plan.

Authentic business continuity planning actually has far less to do with backup technology and far more to do with people and processes. It is not primarily a technology question; it's an operational issue. The "tape guy" is probably not going to be the best person to tackle the job alone.

### Much More Than Technology—BC Planning Encompasses People and Processes

Comprehensive BC/DR involves planning for scenarios, devising processes, and affecting the culture of an organization (versus just implementing better backup or replication). For example, the internal employee-communication component alone is huge, and it has virtually nothing to do with technology itself: A DR plan must be researched, written, and distributed to all applicable departments. Those departments need to be trained on it, and they must practice it with dry runs. This is an effort encompassing more than IT technology.

To be fair, it is IT technology that ensures *data* survivability; and without data survivability, other BC/DR processes and policies may not even matter. That's probably why most people these days are inclined to think about BC/DR in the context of the IT pro who oversees backup.

But it is highly unlikely that the backup admin would know all of the right questions to ask, whom to ask, what procedures to document formally and in what detail, and all the other processes required to implement a strong, workable BC/DR plan. He simply "doesn't know what he doesn't know."

It takes a specific mindset *and experience set* to be able to step back far enough to get an all-encompassing view of the organization, and then dig deeply, scrutinizing the core business processes that the company depends upon. Fundamentally, it takes a "different kind of human" to:

- Quantify the cost of downtime for each mission-critical and business-critical process.
- Assess what mitigating technologies could be used to reduce the downtime risk or downtime duration.
- Define, draft, and validate a plan leveraging those technologies and integrating them into the daily culture of the organization.

BC/DR management is essentially a different occupation *altogether*. It's not tantamount to the person who's standing in a corner of the glass house each morning swapping tapes.

### Don't Think Bits; Think Dollars

Because business continuity planning is less about backing up, doing snapshots, or replicating, and far more about understanding the cost of downtime, lost productivity, and lost reputation, it is, by definition, an operational discipline.

In fact, in almost every case, the first step involves converting technical challenges, bottlenecks, and potential-crisis moments into operational processes that are financially quantifiable.

For example, a server going down is not the bottom-line problem. The problem is that when that server goes down, a certain department is affected, which costs the company "x" dollars. It is a financially quantifiable situation. Outages, service-pack updates, hot fixes, and disrupted backup schedules all have a particular dollar-loss value. One must figure out what technologies and processes to deploy to reduce the amount of loss.

In some cases, the biggest challenge is understanding the many

**BUSINESS CONTINUITY PLANNING** is far less about how you are going to back up, snap, or replicate, and far more about understanding the cost of downtime, lost productivity, and lost reputation.

BC planning is an operational discipline, not a technology-focused one.

interdependencies between various applications and the departments that rely on them. Some organizations may find that they need business continuity planning software that has been engineered specifically to help them understand and document interdependencies across an infrastructure.

On that note, as part of its effort to analyze [Sungard Availability Services'](#) broader portfolio, [ESG also recently investigated Sungard Availability Services' BC Assurance software.](#)

## Backup Isn't BC/DR, and the Skills Aren't Synonymous

So, the challenge centers on expertise, and “a different kind of human” should be taking on the BC planning role. But the reality is that there aren't enough authentic business continuity experts to go around. In particular, there aren't enough BC experts who are willing to come on board to a midsize organization that will probably ask them to perform myriad non-BC/DR duties as well. A midsize organization, frankly, can't justify a full-time business continuity planner.

Although midsize organizations should place a very high priority on improving BC/DR preparedness, they usually have to gain access to the expertise they require via BC/DR consultants and service providers. Respondents to one recent ESG research survey acknowledged this gap, with 65% of midmarket organizations reporting that they do not have enough employees on staff who are skilled in BC/DR (see Table 1).<sup>4</sup> As mentioned, the gap is more evident in midsize organizations than in enterprises, but midsize organizations are, unfortunately, more constrained in regard to actions they can take to close the gap.

Although the survey focused on skill gaps in relation to virtualization goals specifically, the findings indicate that the midmarket's current BC/DR focus has had a side effect. It is revealing to these organizations that personnel presumably responsible for supporting BC/DR strategies actually do lack sufficient experience, so the company needs to take some type of action.

*Table 1. Alignment Between BC/DR Skill Sets and Virtualization Goals, by Company Size*

How aligned are the BC/DR skill sets of your IT staff with your organization's virtualization goals?		
	By company size	
	Midmarket (100 to 999 employees, N=130)	Enterprise (1,000 or more employees, N=180)
BC/DR skill sets are in alignment with our virtualization goals.	35%	46%
BC/DR skill sets are <i>not</i> in alignment with our virtualization goals, so we will train and educate our existing staff.	26%	23%
BC/DR skill sets are <i>not</i> in alignment with our virtualization goals, so we are actively recruiting resources.	19%	18%
BC/DR skill sets are <i>not</i> in alignment with our virtualization goals, so we will engage with consultants to fill any skills gap.	15%	10%
BC/DR skill sets are <i>not</i> in alignment with our virtualization goals, so we will adopt a managed service approach.	5%	3%

Source: Enterprise Strategy Group, 2013.

Many midsize organizations simply cannot afford to employ a person who is as adept and experienced in BC/DR as they actually need. Or, at least, they cannot afford to bring that person on board permanently because a full-time certified expert wouldn't have enough BC/DR-specific work to do to warrant being onsite 40-plus hours per week.

<sup>4</sup> Source: ESG Research Report, [Trends for Protecting Highly Virtualized and Private Cloud Environments](#), June 2013.

And it's likely that a legitimate expert isn't going to be professionally fulfilled for too long by doing other kinds of routine, tactical activities to fill up the average day.

So, midsize organizations often opt for a part-time or outsourced resource (if they make a staff-related commitment at all). It is actually a good solution to a tricky problem. With an outside resource, the organization does not have to allocate a large annual salary to someone who won't be busy all the time or who would be unhappy being saddled with other IT administrative chores. And when they outsource the BC/DR oversight role to experts, for example those at a company such as Sungard Availability Services (AS), they get the advantage of being supported by some of the top BC/DR specialists in the world.

## The Best Part of BC/DR Is the Preparation, not the Recovery

The "best" part of BC/DR has little to do with how recovery exercises unfold smoothly and successfully following a disaster. Rather, the best part of BC/DR is uncovering "ugly truths," operational inefficiencies, and legacy components during preparedness and planning efforts beforehand. In BC/DR planning, experts have to look, with fresh eyes, at *everything* in the environment. And that means questions start to arise, such as:

- How important, really, is this business process?
- How important is that application?
- Does anyone still use this server?

From there, questions follow intended to lower the probability that important apps and processes go down:

- Is the app sitting on the proper hardware?
- Have we updated to the latest software version to ensure recoverability?
- What other apps or processes does this one interact with or depend on?
- What happens if *they* go down?

You may find that no one uses some applications anymore; you can stop backing them up and start shutting them down. You may find a newer software release of the application exists, and the new release will let you leverage the cloud for native high availability; those backups can cease, too. On the other hand, you may find an application you thought was in test phase actually has 100 users depending on it every day to do their jobs. You'd better implement a recovery scheme, and fast.

Invariably, using fresh eyes to reexamine an architecture allows you to gain efficiencies. You figure out what servers are underutilized and candidates for virtualization. You uncover servers that are overutilized, so you move some apps residing on them to different platforms. Basically, you uncover all kinds of operational improvements that you can implement to allow IT to function better even if nothing fails. In other words, the benefits arising from BC/DR planning are solid even when no crisis happens.

That's the good news.

The bad news (as mentioned earlier) is that this fresh-eyes reexamination demands a kind of expert who is not the "backup guy." The expertise you're looking for comes in the form of a high-level **infrastructure architect** who understands business processes, BC/DR concepts, and secondary-site implementation technologies—a person with a skill set extending far beyond backup, and yet mindful of recovery.

It should be clear by this point that BC/DR planning is very important, but the average backup admin isn't suited to lead the charge. So then, who is?



## Sungard AS Recovery Services

When considering “expert” brands in BC/DR, one of only a few names to surface is Sungard AS.

Sungard AS is a company with a strong pedigree as a traditional BC/DR provider. But in many cases today, companies are not looking for Sungard AS to become their alternate cold site. Rather, they want an expert’s fresh eyes and experience in devising, testing, and culturally “indoctrinating” a solid BC/DR plan into their organizations.

Although Sungard AS has traditionally been the complete BC/DR failover provider for large enterprises, it seems to recognize midsize organizations’ ever-growing resiliency needs, ever-maturing IT infrastructures, and lack of expertise and secondary locations. With more than 30 years of BC/DR expertise and an ability to leverage the mainstream availability of “cloud” services, Sungard AS is promoting a holistic approach to application availability, offering prospective midsize clients the opportunity to use its experience and infrastructure.

### Application Availability

Two interrelated offerings—Sungard AS Managed Recovery Program (MRP) and Sungard AS Recover2Cloud—enable Sungard AS clients to pursue a holistic approach to providing infrastructure, application, and data support utilizing Sungard AS’ proven people and processes.

#### ***Sungard AS Managed Recovery Program***

With its Managed Recovery Program, Sungard AS aims to help its clients:

- Achieve and ensure a constant state of readiness for their mission-critical applications.
- “Optimize” the cost of IT recovery management and improve recovery performance.
- Put a robust recovery program into place.
- Refocus their IT staff on business value creation.

Key deliverables of the program include:

- Application technology and configuration mapping: A map depicting a holistic view of applications, including interdependencies, infrastructure, storage, and peripherals.
- Recovery procedure documentation: Comprehensive work instructions for restoring hardware, operating systems, and application data.
- Testing program execution: MRP testing and recovery plans provided after application data has been restored.
- Post-test reporting: The post-test report covers goals, objectives, and achieved results—as well as providing opportunities for improvement.
- Configuration and procedure lifecycle maintenance: Ongoing identification of production changes affecting DR configurations, including ongoing updates about those procedures and configurations.

Assuming that a Sungard AS client responds appropriately (i.e., taking the proper steps to make the most of those deliverables), then that client should expect to see cost savings, reduced RTOs, better productivity and focus from the IT staff, and in an overall sense, an improved “steady state of readiness.”

#### ***Sungard AS Recover2Cloud***

At the core of the Recover2Cloud service suite is an ability to select from a variety of offerings with defined recovery objectives, varying levels of automated failover, and execution at the server/virtual server and storage infrastructure layers. These services are designed to address a range of recovery point and recovery time objectives at different investment levels to match a typical tiered-applications environment. The suite currently includes three service options: Recover2Cloud for Server Replication, Recover2Cloud for Storage Replication, and Recover2Cloud



for Vaulting. The service options are well aligned with how organizations classify their applications, from “mission-critical,” to “business-critical,” to “best effort.”

Common components for all offerings include:

- Sungard AS’ cloud platform, offering a standby site that is fully managed to deliver rapid restart and availability of applications when disruptions and failures occur at the primary site.
- Replication of data to Sungard AS’ cloud using standard technology components such as storage system replication, host server replication, and online backup software.
- A subscription-based model with the rates structured on the number of VMs or physical servers that are protected (with a possible additional charge for storage consumed, based on specific Sungard AS services). In any event, customers do not need to buy dedicated infrastructure.
- And as a rare occurrence in the data protection industry, Sungard AS offers a service level agreement guaranteeing that the recovery time objective defined in the offering will be met if the primary site fails.

In each Recover2Cloud service, a customer establishes an application environment to copy or replicate to the Sungard AS cloud. When a failure at the primary site occurs, Sungard AS orchestrates a failover operation reconnecting customers with the replicated environment.

Essentially, Sungard AS has extended from offering only warm sites for enterprises to offering cloud farms for the millions of midsize organizations that need them, while continuing to build on its core competency—namely, assessing, planning, testing, and delivering BC/DR preparedness. For that whole segment of midsize organizations that previously perceived BC/DR preparedness as being unattainable, Sungard AS intends to help them overcome the two presumptive blocks: lack of expertise and lack of redundant infrastructure.

### **How Sungard AS Is Redefining BC/DR for Midsize Organizations**

Instead of just talking to the technology people—those personnel (many of whom are either backup administrators or IT generalists) who have been trying to be the “part-time” disaster recovery and business continuity people within their organizations—Sungard AS is talking with all the right people about the impact that availability has on the infrastructure, applications, data, end-users, and processes that together make up a midsize business.

Sungard AS reports anecdotally that after it signs up a midsize company for a service and starts the discovery phase with that client (examining the environment, writing test scripts, etc.), the Sungard AS specialists often find that what the client believes are the critical applications or dependencies—the things the client needs to protect most—have not been ranked in the right order.

It’s why some Sungard AS project managers tend to take a “failure-mode-effects analysis” approach. Although certain absolutely business-critical applications and services are “no brainers” for placement at the top of a recovery list, other factors—such as reputation/credibility loss—weren’t even considered. Sungard AS helps these companies weigh the potential of bad financial impact to determine holistically what the applications needing BC/DR coverage are, what order and ranking they should be prioritized into, and even how to move those apps away from a “DR scenario” and into a cloud or an always-on environment truly centered on recoverability.

## The Bigger Truth

Business continuity planning is more about people and process than technology, so BC/DR efforts shouldn't be led by IT teams alone ... especially not by backup people alone. This is a job requiring different skills—skills that, in a midsize business, are hardly ever internally nurtured as a full-time position.

But even though midmarket companies have less expert support on hand, they need business continuity and disaster recovery planning expertise *more* than larger enterprises do. After all, they usually don't have the latest and greatest high-availability products integrated into their environments, and they don't have "Clark Kents" dedicated solely to keeping their eyes on all things, always ready to pull on their capes and maximize the chance of fast recovery from a disaster.

Even if a midsize company *were* to come up with enough budget to retain a certified BC/DR expert full time, the best specialists wouldn't likely be interested in working there. The chance is too high that they would end up stuck splitting their time between true planning and mundane IT tasks.

A BC/DR expert is a "different kind of human." Some midsize organizations already understand this. That's why they will often seek outside experts such as Sungard AS to partner with them on an ongoing basis to develop and maintain an overall recovery strategy. Proper business continuity and recovery planning—not to mention the efficiency benefits they will gain on a daily basis—are just too important to ignore.

And after midsize organizations have "solved" their expertise issues and developed a BC/DR plan, some will determine that they'll also need a different kind of infrastructure solution to host their BC/DR IT resources. Those folks will probably be happy to remember that Sungard AS does that, too.



Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | [www.esg-global.com](http://www.esg-global.com)