White Paper

Five Steps to Achieving Business Continuity for Everyone

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.

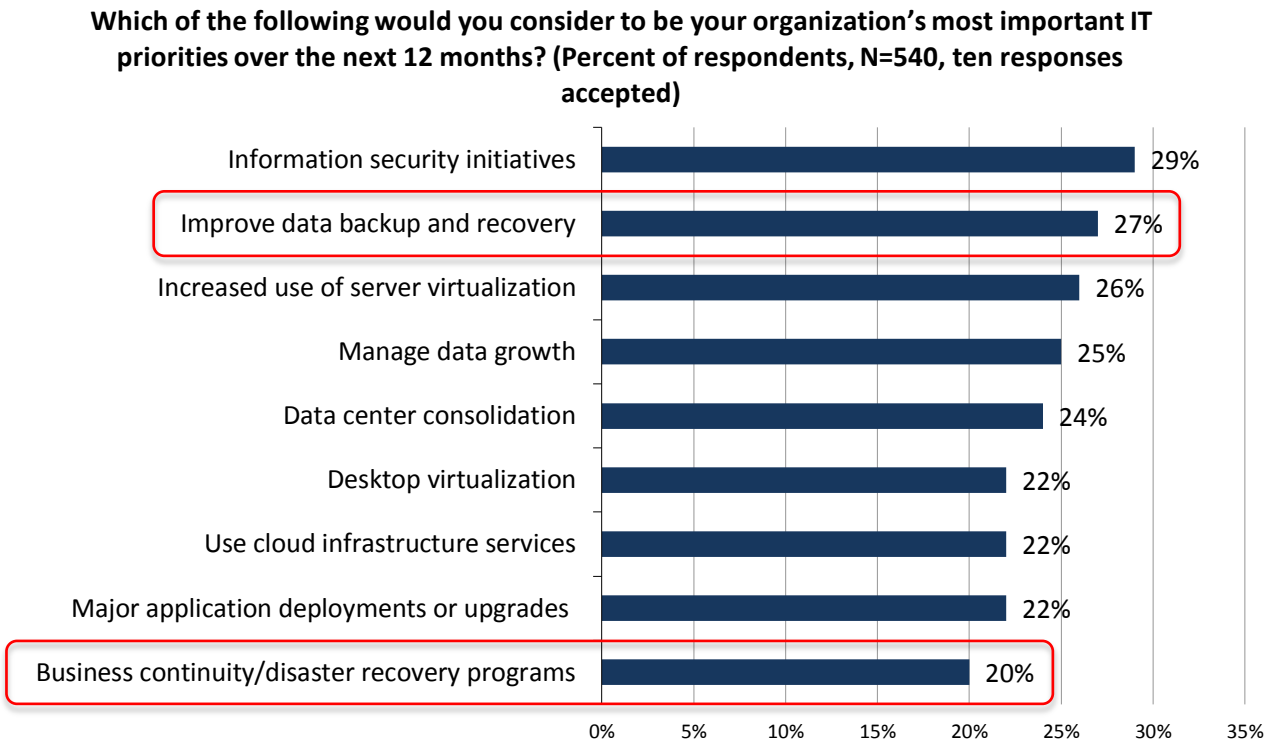
Contents

Business Continuity Planning Is Vital

In 2012, as part of a research survey, ESG asked IT professionals what specific data protection challenges they were facing.[1] Thirty-six percent of the respondents indicated that implementing or improving business continuity and disaster recovery was a process and technology challenge they faced. Interestingly, 32% of them also cited a lack of a disaster recovery plan or process as a challenge they wanted to overcome.

Professionals working in the IT organizations of midmarket and large enterprises alike continually cite improving backup and recovery as a major strategic priority. In ESG's *2013 IT Spending Intentions Survey*, for example, improving backup and recovery was the second most commonly selected IT priority among respondents, with BC/DR programs also making a prominent appearance in the priorities response list (see Figure 1).[2]

Figure 1. Top Nine Most Important IT Priorities for 2013



Source: Enterprise Strategy Group, 2013.

Considering the recurrent (some would say persistent) presence of backup and BC/DR in these ESG research lists of IT challenges and priorities—year after year—most people would agree that it's no easy matter to nail down a rock-solid disaster mitigation strategy "once and for all." The goal, of course, is to develop and deploy a plan that is tested, vetted, accepted, understood, and participated in by all affected employees.

The plan must be comprehensive, and most importantly, it must work exactly as prescribed, regardless of minor service outage or worst-case scenario, with all plan participants (IT pros, BC specialists, business leaders, etc.) knowing their roles and performing their predefined tasks.

Yes, it's hard, but it is necessary. Virtually no business is immune to the threat of interruption. And those interruptions can come in all shapes and sizes.

[1] Source: ESG Research Report, *Trends in Data Protection Modernization*, August 2012.

[2] Source: ESG Research Report, *2013 IT Spending Intentions Survey*, January 2013. Business continuity/disaster recovery programs were tied at 20% with regulatory compliance initiatives, business intelligence/data analytics initiatives, improving collaboration capabilities, and deploying applications on or for new mobile devices.

More Than Floods and Fires: A Good Mitigation Approach Spans a Wide Range of Possibilities

A water main break, gas main explosion, ammonia leak, wind storm, blackout … pick your poison. Many catastrophic events have the potential to disrupt business continuity. But BC/DR discussions shouldn't center on recovering only from "traditional" major disasters. Small-scale outages, including outages limited to one campus building or even one rack of servers, are just as likely and possibly just as harmful to operations.

Likewise, the practices and methods involved in business continuity planning apply regardless of how broad or small the scale of business operations is, or how big or small the data center or remote office might be. Business continuity is about people and processes as much as it is about technology.

But the most important thing of all to know is that regardless of what you might presume about how expensive mitigating technologies, availability solutions, and BC planning efforts are, *the cost of downtime will inordinately exceed those expenses*.

Changing the View—Establishing a Holistic Business Perspective

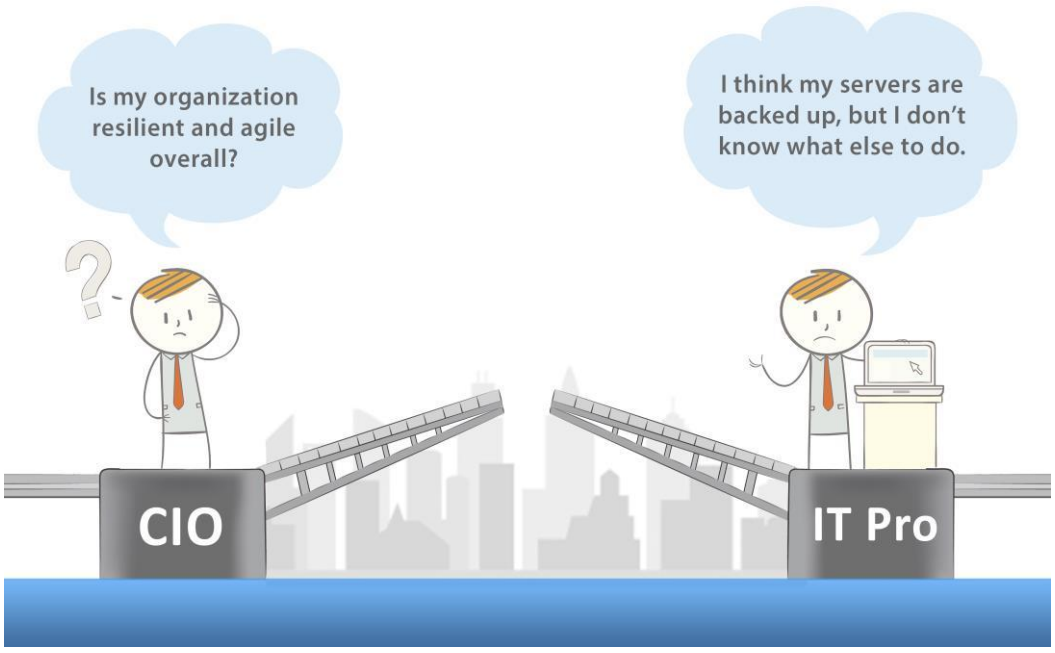
In organizations of most sizes, the CIO likely does not have a high level of confidence that the IT team could recover key data-related business processes quickly following a calamity of any size. However, that lack of confidence is usually *not* due to doubts that the IT team is capable: CIOs know that their IT departments are quite competent.

> IT pros don't know what answers to prepare. And CIOs don't know what questions to ask.

Rather, most CIOs do not have enough information at hand—whether in writing or through computerized dashboards—to gauge that team's preparedness and thus feel that sense of reassurance. As a result, many CIOs presume the worst.

The lack of "sureness" goes both ways. The CIO does not know whether the IT team is prepared. The IT team doesn't know what information the CIO needs to be furnished with to feel confident about the organization's BC/DR preparedness. In other words, the IT professional doesn't know what answers to prepare and provide, and the CIO doesn't know what questions to ask. Neither one knows how to talk to the other (see Figure 2).

Figure 2. They Don't Talk to Each Other Regularly, and They Don't Talk to Each Other About the Right Topics



Source: Enterprise Strategy Group, 2013.

Additionally, the gap isn't limited to the CIO and IT pro. Larger organizations with separate functions for risk management, internal auditing, and general IT often suffer from a lack of common tools and sharing mechanisms. Everyone has faceted and inconsistent views of the organization's overall preparedness as a result.

In some organizations, particularly those that haven't previously invested in authentic BC/DR preparation, the best way to figure out the right questions to ask may be through the use of specialized consultants—not generalist IT professionals or even backup administrators, but folks whose expertise lies in developing and enacting BC/DR strategies.

Who Is Your BC Professional?

With many technology-enabled business discussions, it is easy to oversimplify the participants as if they belonged in one of three buckets: "IT professional," "non-technical business owner," or "user of the systems."

However, a fourth role should be recognized and understood when considering proper BC/DR preparedness: the "business continuity professional." A BC pro is someone who can help the other participants answer questions such as:

- What are the business impacts or costs associated with the BC/DR plans (or the lack thereof)?
- How effective are the mitigating plans and mechanisms in protecting the productivity of the business?
- What needs to evolve or change for the organization's requirements to be met initially and remain satisfied?

Although not always represented as a full-time role or officially titled individual (internal or external to the organization), the BC pro is key to helping teams bridge their understanding and communicate their needs so that the whole organization can plan for assured productivity.

You Don't Know What You Don't Know

Part of the BC planning process is to look *holistically* at business processes and their underlying IT delivery mechanisms. Challenges abound in understanding the various IT mechanisms, their vulnerabilities, and the opportunities to strengthen their availability.

Challenges in Discovery

Discovery-related challenges center on being able to identify all the core IT platforms that various business units use. Often, departments and whole organizations may appear as a cluttered, undocumentable meshing of a range of user groups and disparately associated IT assets. It's usually not realistic to expect to line up a finite group of users and a finite group of IT assets; in the real world of business, everybody shares resources to some degree.

Also, "rogue" systems and applications might be consumed directly by the business, and IT has little visibility into or control over what is actually happening over time.

Regardless of organizational size or decentralization of IT assets, the "Who is dependent on what?" question remains. When that question can't be answered, quantifying and protecting the resources becomes inordinately difficult.

Challenges in Change Management

Without a proper understanding of the user and business-function dependencies tied to a given IT asset, it is extremely complicated to recognize, document, and plan when change-management scenarios should unfold. For example, an IT resource is taken offline for what is supposed to be a benign update or maintenance task. But that effort happens at a time of the day or quarter when key users or business functions depend greatly on the resource. The productivity of those users is therefore impaired, sometimes seriously, by the purportedly "routine" operation.

Challenges in Expertise Sharing

A couple of challenges, or more specifically, gaps, exist relating to IT organizational expertise and BC/DR:

- One is an internally created gap in which two or more peer workers don't have time or aren't properly motivated to share all relevant information necessary for them to do their jobs. This gap may encompass not only peer IT professionals, but also IT pros and the business stakeholders who depend on them. When employees aren't sharing everything they know, it limits productivity and hampers the collective ability of everyone to execute on the company's strategic mission.
- The second type of expertise-sharing gap arises when *no one* in an organization has the insights or expertise to aggregate the needs, constraints, and goals of company groups such as IT, risk management, legal, and various business units. In this case, even if knowledge is shared thoughtfully and frequently between business stakeholders, IT pros, and executive management, the expertise gap remains because experience in proper joint BC/DR planning literally exists nowhere in the organization. This situation is particularly observable in midmarket businesses and even in smaller enterprise-scale organizations, and it reinforces why ESG sees these organizations often seeking BC/DR-related expertise in the form of ongoing partnerships with outside consultants. (The new ESG white paper *Redefining BC/DR Planning for Midsize Organizations* is available from Sungard Availability Services and contains more insight on this topic.)

Challenges in Business and Process Alignment

The challenge in business and process alignment also equates to a type of gap—but this gap centers on lapses not only in intra-organizational communication, but also in infrastructure-related uncertainty about the relationships among business processes and the underlying dependent technologies and architectures. No one is focused on tracking all the changes in configurations made to accommodate new initiatives, changes in corporate focus, etc. It's an ambiguous endeavor to be sure, and admittedly, without the right tools, the job is absolutely daunting.

Changing the Culture—Making Preparedness a Part of Production

Backup as an IT process does not actually affect corporate culture. (It should, but it doesn't.) Production architecture and operations, however, *do* affect corporate culture, while backup "just makes copies of it."

If you developed a BC/DR plan but it hasn't affected corporate culture, then that plan became out of date the day after you published it.

A successful BC/DR plan makes preparedness part of the culture of production.

If you've developed a BC/DR plan but it hasn't affected corporate culture, then that plan became out of date the day after you published it. Why? Because the production environment changed. New servers were added; machines were moved; the criticality of services changed.

Production changes. If you haven't made preparedness part of production, then when those production-environment changes inevitably happen, they won't be organically reflected in your preparedness plan. And when it comes time to failover, you won't be able to completely—because you didn't know about the servers and services that were added after you finished your (static) plan. Your preparation effort stopped the day your plan was published. The "perpetual changing" of production IT is a key reason to increase communication and collaboration among BC/DR stakeholders and use investigate tools that can monitor for IT changes, so that the BC/DR plan can continue to evolve.

Other things to consider:

- Executive sponsorship is needed to make sure that business continuity really does affect culture. A backup administrator isn't going to be able to affect the culture of the IT team, much less the culture of the whole business.
- In many cases, the backup admin does not have enough information to know, as production changes, what corresponding changes the BC/DR plan needs to receive. However, tech tools can help. Such software

solutions can assess what's on the wire through discovery and communicate to the admin what the interdependencies are. That's something very hard to figure out with spreadsheets alone … but by using the *proper* tools, IT knows just how production is changing and thus can sustain and evolve the BC/DR plan accordingly.

Preparedness has to be part of production, and it is a cultural change dependent on a technology-level understanding of what is in, and what is evolving within, the IT infrastructure.

Evolution from IT Recovery to Business Resiliency = Your Evolution to BC/DR Strategy Leader

The journey from IT backup (which is often tactical) to business resiliency (which is more strategic) is part of an even bigger conversation about moving professionally from the tape closet to being an advisor to the CIO. If you are affecting culture, then you are leading. A backup administrator manages. A BC/DR infrastructure architect leads. A manager is tactical; a leader is strategic.

A backup administrator *manages*. A BC/DR architect *leads*. Do you want to be a manager or a leader?

When you start thinking about ways to affect culture, to convert technical challenges into business challenges and solutions, that's when you go from being a "manager of backup tactics" to a "leader of BC/DR strategy."

How to Understand What You Have, So You Can Protect It

Now that we recognize that we are engaged in a process of converting technology challenges into business challenges, and we know that what is limiting us is being able to monitor and evolve with production, what's left?

People need a state-of-the-art way to track everything. In the *really* old days, they did so on paper (albeit big, ugly, marked up sheets of paper). Later, companies used business continuity planning tools that allowed them to create and modify BC/DR templates electronically. But that was still an archaic approach akin to filling in forms; the mechanics really were not too different.

Business continuity planning tools have undergone a tremendous evolution. Today, what IT should look for is not necessarily an electronic "form" that documents a process, but something that constantly maps back to the actual organic, ever-changing IT infrastructure. In 2013, it is reasonable to expect that the same tool able to help IT develop a BC plan ought to be aware of the infrastructure components included in that plan. Organizations should look for tools embodying the expertise of BC plan formulation—tools that are usable by non-BC/DR experts to start their planning.

Consider a tax-preparation software analogy: A lot of people who once took their receipts and records to an expensive accountant each year no longer do. Today's user-friendly tax preparation software walks them through a series of questions and provides them with sufficient information in written and graphic form to enable them to prepare their own returns. Of course, just as tax software did not spell the end of accountants everywhere, BC/DR planning software may need to be supplemented with BC/DR experts (based on the organization's complexity and infrastructure).

The same way that tax-prep software revolutionized the process of filing income tax returns, business continuity planning software encapsulates all the most common BC/DR concepts. It can move IT—and by extension, all the non-BC/DR experts in the company—a significant way forward.

Now That You've Planned It, the Plan Must Live

With a clearer understanding of your infrastructure and your users' dependencies, you can craft your BC/DR plan. But after that's done, the question becomes, "*Is our plan alive*?" Regardless of the scope of an incident or outage, will your plan be effective in prescribing the appropriate actions and ensuring that the right people have what they need to ensure that your business continues?

The same evolutionary leap from paper receipts and forms to tax-preparation software (still typically used only annually) can be seen again in the rise of financial-management software that one uses throughout the year—software that covers not only taxes, but also retirement savings, college savings, bill payments, etc. That same evolution is occurring with software-based BC/DR templates becoming living BC/DR plans that, ideally, adapt easily in tandem with the actual production environment.

It cannot be overstated that BC/DR planning is not a one-time activity (even simply to satisfy auditors). In the same way that a modern financial tool might alert you about an imminent overdraft, modern BC planning systems guide you to the right actions and reports based on the current status—upcoming regulatory audits, weather alerts, etc.—of a properly prepared environment.

When it comes to modern business continuity planning software, look for a product integrated with—i.e., able to access and discover—the actual IT infrastructure. The best products don't just offer a plan for its own sake; they evolve as the infrastructure evolves, capturing the "plan of the moment" from both a technical and business perspective.

Sungard Availability Services (AS) BC Assurance Software

One such product is Sungard Availability Services BC Assurance software. This product removes barriers to organization-wide BC/DR engagement and boosts everyone's confidence in the preparedness plan. It addresses compliance requirements, and more, to truly prepare teams to recognize threats to the business and empower them to act before small incidents lead to major disruptions. Organizations that need more than software can turn to the Sungard AS Managed Recovery Program for an even deeper level of consultative support or services.

The Five Steps to Getting Started with BC Planning

BC planning is something that everyone should be doing, just as personal financial planning is something that everyone should be doing. But frankly, without a tool that is accessible and understandable, most people don't. They're too intimidated. When things are too hard, you tend not to do them, even though you know you should.

The following steps represent ESG's prescriptive guidance to assist an IT professional who is interested in *really* getting serious about business continuity planning.

Step 1: Don't wait for the plan to be finished before you start deploying BC/DR efforts.

If you wait for the plan to be "finished," you'll never enact anything because BC/DR plans are living things. What unfortunately happens to people who wait is that their organization actually does suffer an outage or disaster, and all they have in terms of preparedness is two-thirds of a plan. They're as dead in the water as if they didn't have any plan at all. Recognize that short-term actions can be taken almost right away, and a longer-term plan will follow to address the "big-ticket" activities that involve culture change.

Step 2: Understand that IT alone cannot do BC planning.

Authentic BC planning includes business-unit stakeholders, application owners, core IT operations, and likely, representatives from the legal, risk management, regulatory/governance/compliance, and HR departments. The planning team also includes an executive sponsor to empower culture change.

Begin by building consensus. You may not have all the answers figured out, but at least you can start assembling a list of questions covering all the applicable people and departments.

- **IT pros**—You may understand the servers, but are you confident that you understand the dependencies and usage patterns between the users and the application services? In addition to assessing technical resiliency mechanisms, start looking for who is using what.
- **CIOs**—The culture shift involved in instilling the disciplined mindset that *preparedness should be part of production* won't happen without your visible sponsorship and ongoing advocacy of BC/DR preparation.

- **BC pros**—The IT pros, CIO, business unit leaders, and application owners all need your help to see the others' points of view and translate the others' taxonomies, presumptions of criticality, infrastructure dependencies, and service expectations.

Step 3: Start assessing the most critical systems.

With the guidance of BC/DR planning software, assess the most critical systems, measuring the cost of their downtime and quantifying the likelihood of downtime against various large and small outages. For example, what are the top three systems the organization absolutely depends on? E-mail? The accounts receivable system? The shipping software? The content management and collaboration platform? Those "big ones" vary from one organization to the next, but all organizations have them. Now, calculate the cost in downtime and lost productivity to gauge the impact to the organization should those systems go down.[3] In some cases, the losses could be in the tens or hundreds of thousands of dollars.

Apply that quantification against big and small outages. If one server's hard drive fails, how long would that outage likely be? If your headquarters sits in the middle of a region-wide power failure, what would the quantifiable loss from that outage be?

You've now done a risk assessment and a business impact analysis, identifying the main things important to the business that could break and the statistical possibility that such breaks will happen. The likelihood that a blizzard will affect operations at a Minnesota-based company is higher in January than in June, for example. The likelihood of one hard drive failing is much higher than the likelihood of a statewide electrical outage. That hard drive outage won't be as "big," but it will happen much more frequently, so one of your first steps should be to mirror the drive. Remember Step 1—don't wait for your BC plan to be "all finished" before you start implementing it. To do this work:

- You need business planning software that discovers your environment and helps you document that environment and your plan for each one of those systems, services, and servers you identified earlier.
- You need expertise. In some cases, that expertise is encapsulated in your availability software. In other cases, it will be in the form of consultants from firms that specialize in BC/DR planning.

Step 4: Implement the tactical changes necessary to mitigate the most common system failures.

At this stage of the effort, you're deploying small mitigating technologies to increase your recovery agility. Examples might include deploying improved storage replication or backup/recovery software that has a higher success rating than what you'd been using. Document those changes in the plan you are developing, and test the deployments to make sure the anticipated improvements occur.

Step 5: Test the plan.

On a predefined, non-negotiable, recurring basis, test the plan for effectiveness and usability. Document the results. Too many people don't want to report failures in their BC/DR tests because they think it's a "bad" thing. Actually, the *best* thing that could happen is a failure during a test because now, you know what to fix. And if you don't document it—and everyone thinks your BC/DR plan is "all green"—they'll be unpleasantly surprised when the recovery effort doesn't work during a real crisis. In fact, it's safe to say that if everything looks green on your BC/DR tests, then you almost certainly didn't test thoroughly enough.

[3] A formula for calculating the cost of downtime is available at http://www.dataprotectionbible.com/images/DP4VDC%20Sample%20Chapter%202.pdf, p. 27.

The Bigger Truth

Legitimate preparedness software must be a big part of any serious, committed effort to prepare for business continuity or recovery after a disaster. You cannot develop an accurate asset inventory using Excel, and you can't develop a living, evolving plan using Word. They're not built for that purpose—designed neither to capture the complexity of IT infrastructure and application dependencies nor the multiple hierarchical relationships among processes and people. Hence, investing in a BC software platform is crucial to success.

You need a solution that provides you with wisdom, clarity, structure, and discipline beforehand; that allows you to enter details germane to your environment; and that folds everything together in a way that gives you an actionable prescription for resiliency.

Even with virtualization and cloud-based services now being mainstream technologies, the guidance discussed in this paper is still applicable to self-managed BC/DR solutions, DR-as-a-service scenarios, or traditional warm sites/vaults. And as a reminder, BC/DR preparedness is even more important for midsize organizations than for enterprises. But without planning software or consultative help, it's unlikely that a midsize organization could be successful with BC/DR.

Operational culture must embrace resiliency mechanisms and processes as part of preparedness and part of production—*not* as an afterthought. That means you need *ongoing* buy-in among the senior leaders, the business unit managers, and the technical teams. Miss any of those groups, and your preparedness effort overall will not work. Specifically:

- If you don't have executive sponsorship, the culture will not change.
- If you don't have business unit buy-in, you won't know which applications are worth saving and which aren't.
- If you don't have the right technology solution in place to support you when disaster hits, you won't have data, and the other preparations you made will not matter.

Again, all three elements have to exist. Otherwise, you don't have a business continuity "plan." You have a "hope."

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