Product Brief

Data Protection Should Be About More Than Products

Date: February 2013 **Author:** Jason Buffington, Senior Analyst

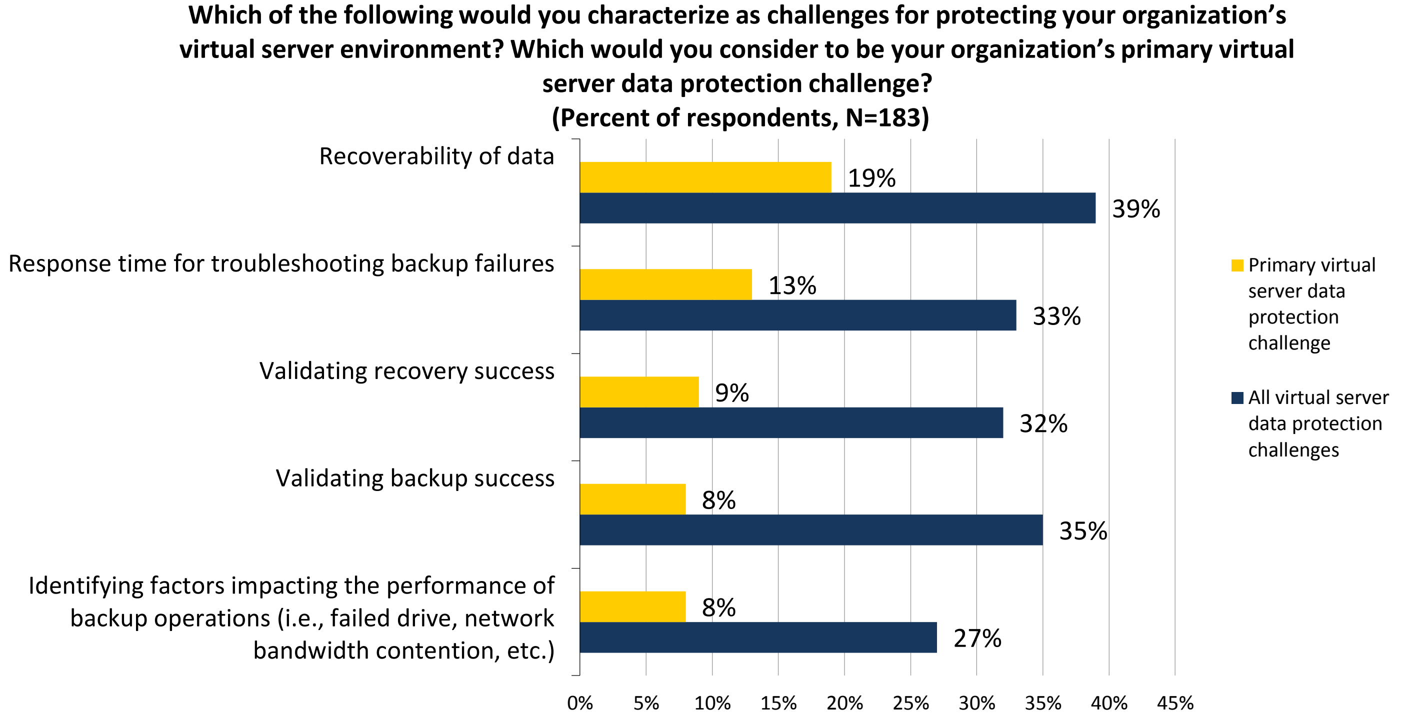
Abstract: *Organizations trying to modernize or fix their data protection capabilities should look beyond the products that they are using and also consider the people and processes required for ensuring successful recoverability. In some cases, the real solution might be to access managed services, which better utilize or optimize the products that companies already have, instead of simply switching products and starting over.*

Overview

According to recent ESG research on data protection modernization, only 86% of backups complete successfully, and only 80% of recoveries complete within negotiated RPO/RTO service level agreements.[1] So, although many IT teams would like to add new recovery capabilities through snapshots, replication, or workload-specific protection tools, the reality is that many still see daily backups as "broken"—with one out of five recoveries not meeting the expectations of their business stakeholders. However, *maybe you do not have to make such a radical change* simply to fix what you already have.

For many, the promise of a new/better technology distracts IT managers from recognizing what is working versus what needs enhancement or resolution. For example, Figure 1 shows the top-five challenges ESG research respondents identified with protecting virtual servers.[2]

Figure 1. Top-five Challenges with Protecting Virtual Servers



Source: Enterprise Strategy Group, 2013.

[1] Source: ESG Research Report, *Trends in Data Protection Modernization*, August 2012.
[2] Source: ESG Research Survey, *Virtual Server Data Protection*, September 2011.

Looking closer at Figure 1, most of the challenges relate to troubleshooting, validating, or identifying, which in fact involve operational issues, not necessarily one product's features compared to another. Said another way, most of the top challenges identified might not be directly addressed simply by buying new products or technologies. The answer lies in how well that technology is being utilized and the processes and practices that are being followed.

Where to Look for Better Backups

You may be currently using an on-premises solution, meaning that you own the storage/servers, and you deploy your own agents. You may be using backup-as-a-service or DR-as-a-service, in which a cloud provider handles the back-end infrastructure, and you license the application agents and pay on a capacity basis. Or, you may have opted for some type of hybrid of those approaches. In each case, the expertise for the monitoring and management of your backup infrastructure still comes from your local IT personnel.

Regardless of On-prem/Cloud, There Is Still a Lot for You to Do

If you are changing your on-premises backup solution to gain benefits tied to economics or new feature sets, then perhaps the change is justified. But before you make a move, consider the effort to solve operational costs related to monitoring, administration, or maintenance—and *think again*. Regardless of whether your solution is on-premises or in the cloud:

- You will still be installing agents.
- You will still be setting, monitoring, and adjusting schedules, upgrades, policies, compliance, patching, etc.
- You will still be troubleshooting backup jobs.
- You will still be invoking data recoveries.

Many of the most common data protection challenges, including those listed in Figure 1, are not necessarily topology problems, nor are they specific to a particular data protection product offering. They are administrative and operational.

Said another way, many IT organizations should spend less time thinking about "what" backup product/topology to use and more time considering "how" or "by whom" their backups should be achieved. For many, backup and recovery challenges are more about the people and processes than they are about the technology.

> Many IT organizations should spend less time thinking about "*what*" backup product or topology to use and more time considering "*how*" or "*by whom*" their backups should be achieved.

Finding the Right "Whom"

The service engagement of others to administer/manage your backup solution while you retain the complete ownership and control of the infrastructure may be what you really need because of the expertise they bring in.

If you are interested in solving the top data protection challenges listed in Figure 1 that relate to monitoring, troubleshooting, validating, and managing your backups and recoveries, then the answer may simply be to have more experienced data protection professionals (DP pros) manage your solution for you—regardless of where your data protection architecture is located. This is particularly true if:

- You have a **significant amount of on-premises backup infrastructure** (servers, storage, and agent deployments) that have not yet returned the ROI they were originally acquired and deployed to achieve.
- Your **existing data protection infrastructure is working nominally** for most workloads and production windows, but it always seems to have minor issues. When the issues are addressed, they are surmountable, but there always seems to be some little thing to fix, monitor, or adapt.
- Your existing IT team members appear to be **taking too much time with ongoing day-to-day management**, even though you are relatively confident in your existing data protection methodology.

- Your existing data protection infrastructure **is not fully depreciated** and still has useful life remaining.
- You are looking to **reduce capital costs and labor constraints** while being asked to improve your data protection service levels or visibility/auditability.
- You have a **small IT team**, and backup/recovery is "just one more thing" on the admin's plate.
- You are supporting **multiple backup sites** and maintaining separate IT teams at each site.

If these situations apply to you, then consider offloading the tactical management of data protection. Like most technology expert areas, DP services experts may come in two varieties:

- **Onsite Backup Administrators or Architects**, which might be brought in at the beginning to solve an ongoing problem or design a new data protection strategy. Like any onsite contractor, while the costs are higher, the return on investment comes with either radically improving the current backup solution (in lieu of replacement) or designing/implementing a new solution without the learning curve or missteps.
- **Remote Monitors and Managers**, providing ongoing monitoring of backup jobs, as well as potentially handling retry jobs, new protection configurations, and restore requests. For the tactical tasks of "backup administration," remote monitoring services may offload the mundane and allow onsite employees to perform more strategic and proactive IT functions.

What Happens to Your In-house IT Backup Experts?

If managed backup services make sense for your organization, it is important to emphasize that your on-staff IT pros who were responsible for data protection will not be out of work. A managed backup service should not be treated as a plot to take away people's jobs; it should be treated as something that augments existing teams' capabilities and that allows the internal IT organization to become more strategic. A vast portion of the time that IT admins used to spend on data protection will be freed up for performing strategic work, and those admins will evolve/mature from *backup people* into *data protection assurance managers*.

> No one has as much invested in ensuring your company's ability to recover as you and your IT team, so your in-house IT team is still crucial for SLA oversight and the vision of your data protection strategy.

So, regardless of the SLAs or other contractual assurances that a managed backup provider or any other service provider may promise, your team is still responsible for ensuring the recoverability of your organization's data. Thus, the person who used to be most familiar with the backup/recovery SLAs that were achieved should now be responsible for holding your managed backup service provider accountable to that level of service, at least. This effort should be based in team communication between on-staff IT pros and managed backup DP pros, as well as dashboards and reporting tools that ensure visibility and accountability by all parties.

This guidance applies, regardless of whether you use an on-premises or cloud-based backup solution.

- **If you use on-premises backup servers,** your IT pros will be partnered with their DP pros, and you can collaboratively deploy data protection topologies—as well as offload the monitoring and maintenance tasks to the DP pros.
- **If you use cloud-based backup services**, your IT team and your managed-service DP pros will still be managing a great deal of the onsite technology, such as production agents, protection schedules, onsite intermediary backup servers, the offsite repository and its quotas, and the overall SLAs.

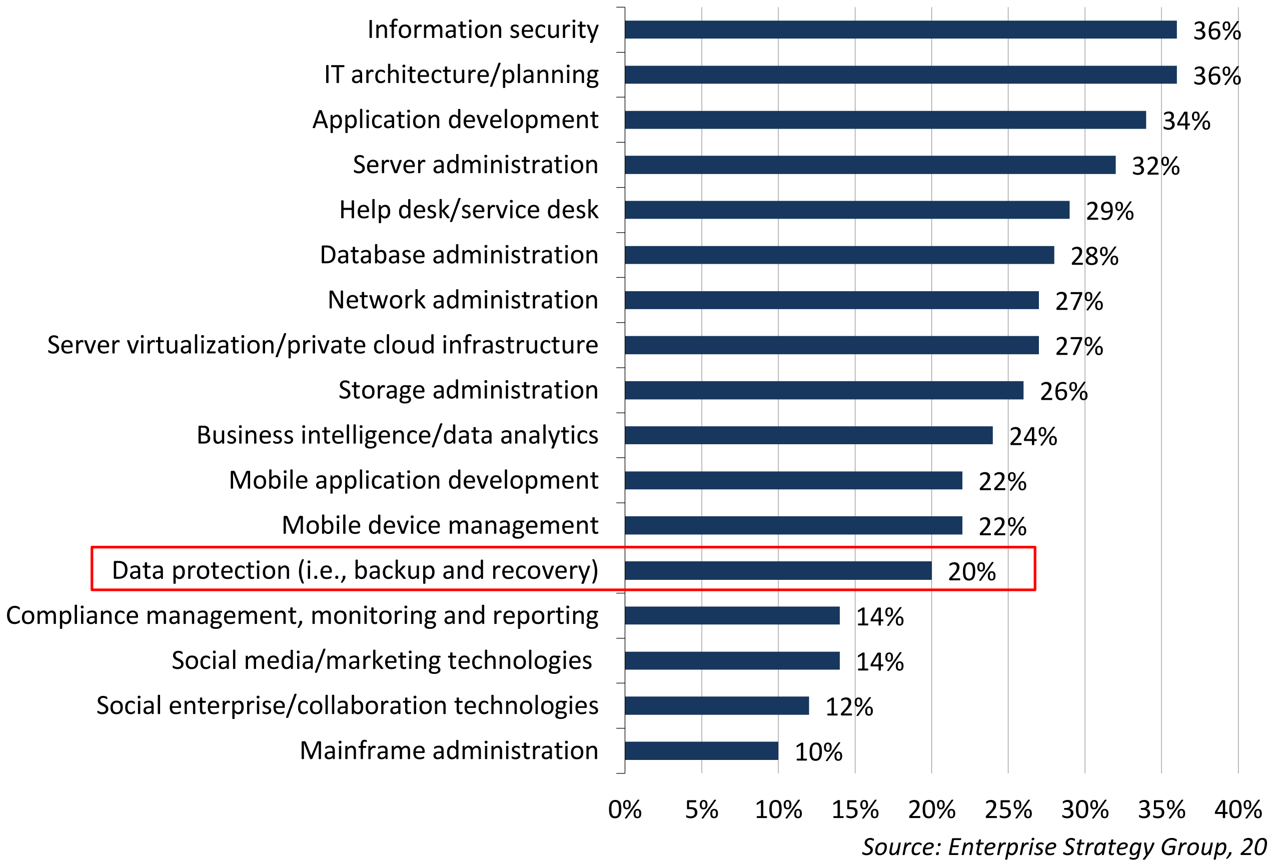
How Managed Backup Services Will Benefit Your IT team

Improving your data protection expertise and visibility through a managed service should yield an improved agility for your IT organization, while your company gets better backup and recovery SLAs without investing in backup skill gaps or personnel within your team. Only 11% of organizations that responded to an ESG research survey said they are planning on investing in *data protection skills* in 2013[3]—making it the 16th most cited response to the question of what skill gaps or hiring commitments are being prioritized within IT organizations. Chances are, in any list, the 16th most prevalent priority will be, relatively speaking, less likely to get done. (And that's an indication of why, generally, IT teams are often overburdened with multiple tactical tasks and lack a strategic perspective.)

By offloading the monitoring and management of data protection to a managed backup service, your virtual IT team members should already be highly skilled in data protection, without your investment or additional headcount. In addition, it is highly probable that when you apply those pros' focused, expert experience, your existing or new backup solution will start to perform better, resulting in higher backup/recovery SLAs for your internal customers, as well as yielding a better ROI/TCO for your backup infrastructure—without a commensurate amount of IT investment from your team.

Figure 2. New IT Staff Positions in 2013

You have indicated that your organization will add new IT staff positions in 2013. In which of the following areas will your organization hire those staff? (Percent of respondents, N=235, multiple responses accepted)



Source: Enterprise Strategy Group, 2013.

As Figure 2 shows, among all organizations, data protection staff hiring ranks in 13th place,[4] which is a relatively deprioritized position compared with all the other roles that IT organizations want to fill. In other words, "other hires are

[3] Source: ESG Research Report, *2013 IT Spending Intentions Survey*, January 2013.
[4] Ibid.

higher." But this doesn't have to be the case. Instead, by offloading the tactical work of data protection to a managed backup service provider, your experienced IT personnel can grow into and satisfy those higher-skill needs.

Symantec Managed Backup Services

With more than 20 years of data protection experience across each of its Backup Exec and NetBackup products, Symantec has long been a market leader in backup. And over the past few years, Symantec has delivered different ways to utilize its software solutions through purpose-built backup appliances, as well as cloud-based backup services. Regardless of whether you manage your own Symantec backup servers, its appliances, or its cloud services, you may also want to consider its Managed Backup Services (MBS).

Symantec MBS was unveiled in mid-2009, targeted at organizations using NetBackup. By offering 24x7x365 monitoring, along with guaranteed SLAs with penalties for noncompliance, Symantec aims to improve its clients' backup and recovery capabilities through improved job monitoring, regulatory compliance audits, and problem escalations through Symantec's own backup experts. Billed as an annual fee, Symantec MBS acts as an administrator of the overall solution, while relying on its trained partners to deliver and implement the necessary actions. In so doing, MBS subscription clients gain the benefits of Symantec's expertise and scale, while not changing the way that they do business with their chosen partners and integrators.

The Bigger Truth

For many people, basic backup and recovery is still "broken."

If you had the time to take a hard look at your problems, you might discover that most of your challenges were not based on technology or product issues, but rather on the operational and administrative chores of data protection. Do reasons exist to change data protection technologies and topologies? Of course. By changing technologies or topologies, you might be able to reduce costs per server being protected, add new recovery scenarios, boost agility, etc. In many cases, it will still be members of your IT team doing a lot of the work related to the new solution, just as they did with the old one.

Adding management services for your data protection infrastructure may very well enable you to solve your existing backup and recovery challenges with minimal new capital investment. In this way, you'll raise your backup and recovery service levels and realize better TCO/ROI on your existing backup infrastructure, while freeing your IT team members from tactical backup tasks so that they can devote more time to strategic compliance or other infrastructure roles.

You might have your own team of in-house backup experts who can handle everything—and have the time to do so. If you don't, it is worth investigating whether your problems (technology or operational) are due to the products that you are using, or the people/processes that are using them. And if so, don't consider changing the "what" (is backing up your infrastructure) before you have first assessed the benefits of changing or supplementing the "who."