Enterprise Strategy Group | Getting to the bigger truth.™

Analyst Brief

SMBs Need Enterprise-quality Data Protection, Right-sized for Them

Date: March 2014 Author: Jason Buffington, Senior Analyst

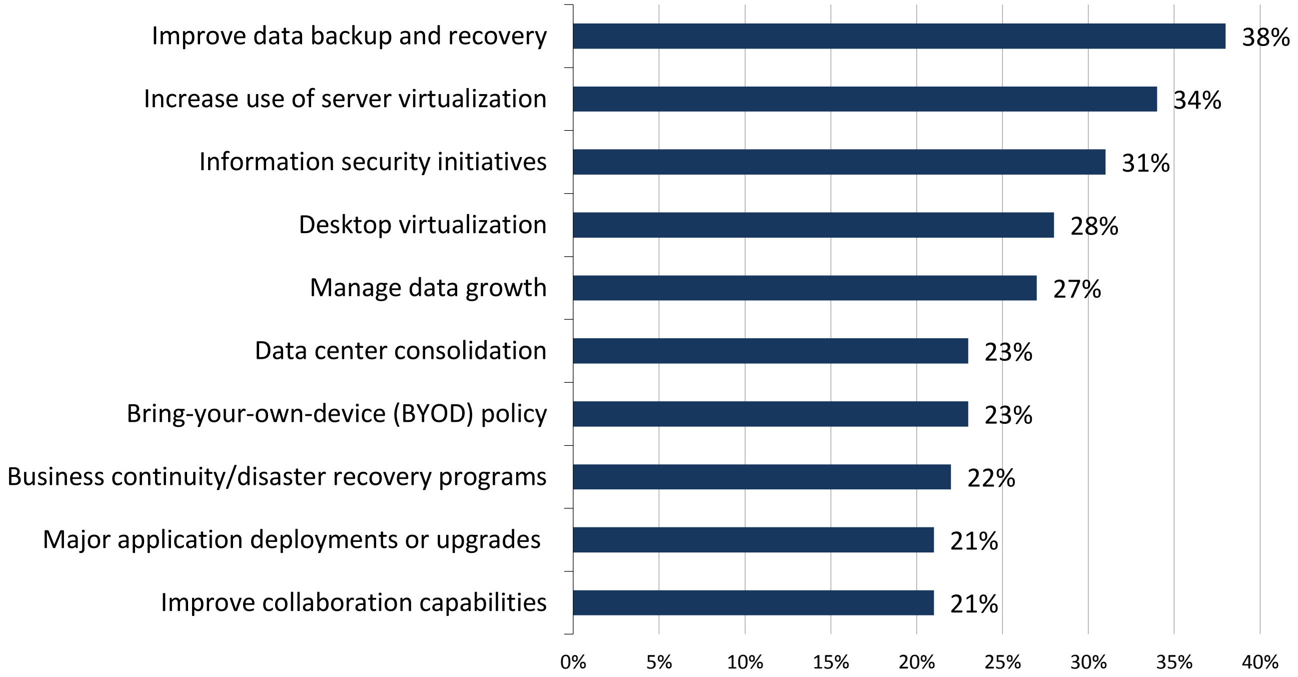
Abstract: *Small and midsized organizations depend on their data as much as large enterprises depend on theirs—but the right tools for protecting smaller organizations' data aren't simply enterprise tools with reduced feature sets and price tags. Organizations of all sizes need to understand the exposure level caused by mediocre protection, and then utilize the "right-sized" technologies that are available in the market today.*

Overview

When a large enterprise has an IT problem, it typically can summon its own onsite expert(s) to fix it. Midsized organizations usually don't have superheroes on staff who can save the day when issues arise. The result is that these organizations suffer inordinate downtime as they try to figure out the problem. Because of this situation, data backup and disaster recovery continue to be high priorities for midsized organizations. In fact, ESG's most recent spending intentions research shows that improving data backup and recovery is the most-cited IT priority of surveyed midmarket organizations for 2014.[1]

Figure 1. Top Ten IT Priorities for Midsized Organizations in 2014

Top 10 most important IT priorities for midmarket organizations (100 to 999 employees) over the next 12 months. (Percent of respondents, N=213, ten responses accepted)



Source: Enterprise Strategy Group, 2014.

For midsized organizations, it is much more efficient to solve IT challenges such as data backup through minor investments in better technologies—and thus avoid major costs due to downtime.

[1] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

Don't Underestimate the High Cost of Downtime

Companies of any size, and the people who make up those companies, rely on their data. Although real data protection solutions are not free, they are extremely cost effective compared with the cost of downtime. Consider a 50-person service-based company with an average annual salary of $60,000 per person:

- Each person earns an average of approximately $30/hour, equating to **$1,500 per hour** across the organization, regardless of whether the employees are productive or not.
- That 50-person company might generate $8 million per year, or **$4,000 per hour** in productivity.

Adding those amounts together, it appears that the simplified cost of downtime for even a small organization could be $5,500 per hour. Now consider the typical server outage:

- Server failures without modern protection capabilities can be estimated to lose ½ a day's worth of data, assuming that the server could fail in the morning (near zero data loss) or at the end of the day (a full day loss). Hence, an average of ½ a day's worth of work is lost, most of which will need to be recreated = **4 hours lost**.
- Server failures without built-in resiliency will typically take most of a business day (best case) to be recovered = a day of limited productivity = **8 hours lost**.

Putting it all together, *a single outage per year can cost $66,000* (12 hours at $5,500 per hour). This model is admittedly oversimplified. Perhaps the organization doesn't come to a complete stop but is instead significantly encumbered when e-mail or file services are offline. In which case, "encumbered" might be perceived as "half productive," resulting in an outage costing $33,000 instead. Of course, your numbers will differ from the example, but the formula and ideas for modifying this cost model can help quantify your cost of downtime.[2]

Beyond just raw downtime, consider the lost customer satisfaction when the company admits that "we can't pull that up right now," or the lost morale internally caused by those impacts or being forced to recreate data that was lost due to an IT calamity.

What Should SMBs Do?

Acknowledging that doing nothing (or something inadequate) will cost your organization significant money, here are some suggestions for how you can help improve your data protection and therefore protect your organization's productivity:

1. Virtualization will improve your ability to protect your data because your servers and services are encapsulated within VMs that not only provide a more thorough protection capability, but also increased agility in restoration scenarios
2. Modernizing your data protection mechanisms will yield more successful backups, more reliable restores, and more flexible recovery capabilities.

Virtualization Is the Great Enabler

Virtualization is a journey that every business environment should be on:

- Some organizations are just starting the journey in order to consolidate underutilized servers or to add new servers/services without adding incremental hardware.
- Some organizations are evolving beyond consolidation toward an agile infrastructure that lets midsized organizations have the same flexibility for new capabilities that enterprises desire—in smaller configurations that make sense.

Regardless of where you are in the virtualization journey, recognize that beyond operational and capital benefits, virtualization enhances your ability to protect your data, and thus your business. Those benefits are so tangible that for

[2] Source: Wiley Press, *Data Protection for Virtual Data Centers*, Jason Buffington, 2010.

most environments (unless there is a technical reason, such as accessing a USB security key or other peripheral), you should continue or accelerate your virtualization journey to the point that you might eventually virtualize every server—even small office servers with only single functions such as file serving.

If for no other reason, virtualize wherever you can because VMs can be much easier to protect. You can easily move a VM from an older or debilitated hardware platform to a newer platform or an alternative location (even a cloud provider's location). Those options aren't possible, much less easy, if you are running your applications or services on non-virtualized systems.

Thankfully, both VMware and Microsoft (through Hyper-V) have economical offerings that provide either a free hypervisor (so you can move your existing OS into a VM), or very affordable virtualization solutions designed for midmarket IT and branch office implementations. A little extra effort to virtualize your server(s) now will yield higher uptime and recovery/agility when you really need it. That being said, be sure to develop your virtualization and protection strategies to complement each other. As seen in Figure 1, virtualization and backup are key priorities, which are habitually adjacent to each other in various annual ESG research results. As such, don't deploy new virtualization technologies without considering the data protection ramifications or benefits—or vice versa. To improve your capital costs through virtualization without assuring adequate protection will reduce your net result if you "put all of your eggs in one basket," but that basket isn't reliable or protected.

Don't Settle for Mediocre Protection

Many people assume that the gap between robust, enterprise-quality data protection and what SMBs can afford is insurmountable. The assumption is incorrect. Don't trust the protection of your data—your business's most precious asset—to scripts, copy jobs, or applets. When selecting one, look for these key capabilities:

- For virtualization protection, **protection solutions** for VMware should leverage the VMware API for Data Protection (VADP) to ensure reliable backups and recoverable data. Similarly, protection solutions for Hyper-V must leverage Microsoft Volume Shadow Copy Services (VSS) to ensure reliable backups and recoverable data.
- **Item-level recovery** is a key capability for both physical and VM-centric data protection solutions. Restores of whole servers after dire events may be why you originally bought your backup solution, but granular recoveries are far more frequently needed. If you haven't utilized those in the past, you and your users will wonder how you managed without it. Not all backup software does ILR well.
- **Deduplication** will save you far more than it costs, period. The deduplication intelligence of when to transmit new blocks versus discard what is already protected can be done within the storage solution, within the backup server, or within the agent/proxy on the production platform – and flexibility is a good thing. That said, effective deduplication should typically be performed as close to the production workload as is feasible, using agent/server approaches over simply within the deduplicated storage, thus requiring a well-integrated combination of software plus hardware.
- **Integrate backups, snapshots, and replication** for even more recovery agility. Each method has its own recovery benefits (e.g., previous versions, rapid rollback, and distance-based recoverability, respectively). The best solutions utilize integrated hardware and software, so that you aren't managing three separate tools within what should be one data protection strategy.
- **Appliances, physical and virtual**, can significantly accelerate adoption and deployment of new IT technologies, including data protection. This includes small offices protecting themselves without necessarily adding hardware, while multi-site environments can replicate from smaller virtual appliances to larger physical ones or to a cloud provider's hosted solution.
- **Predictable performance** for backup windows and restore times is a key to negotiating SLAs between the backup administrator and your business/application stakeholders. Routinely test your recovery methods so that you can provide real-world RPO and RTO estimates to your constituents – and never assume that vendor published backup speeds (if available) are indicative of their performance during restores (or vice versa).

Plan for Tape Plus Disk Plus Cloud

Recognizing that a variety of software is available to help enable your data protection strategy, take a close look at the medium that your "data of last resort" will live on:

- **Disk—**Disk-based storage for backup (and often archive as well) is the ideal medium for many data protection scenarios. It often boasts deduplication, compression, and replication capabilities that enable a broad range of recovery scenarios for midmarket organizations, in form factors and prices that are right-sized. Modern backup software is designed with a disk-first approach, making the combined solution simple to deploy and reliable to use. For most environments of any size, disk is the best medium for first-tier recovery, including both server-/appliance-based internal disk, as well as deduplication storage arrays. Either way, the ability to continually deduplicate and compress redundant data over a long period, along with its performance characteristics in granular recovery, makes disk a recommended basis of most data protection strategies.
- **Tape—**Modern tape solutions, including standalone drives and robotics, still undeservedly suffer from the "tape stigma" of two decades ago. LTO drives boast performance that most single servers will struggle to feed fast enough, while providing a very inexpensive way to store a significant amount of data. Tape data has a shelf-life of many years, and tapes enable users to store or transport that data easily to a vault, secondary office, or the small business owner's home. Thanks to continued innovations such as LTFS, which lets a tape cartridge be mounted and accessed as easily as a USB thumb drive, tape will continue to have a place in a wide variety of organizations. With reliability "solved" in modern tape offerings and recognizing the affordability of tape in terms of best GB/$, tape solutions can be an effective complement to many data protection strategies.
- **Cloud—**Data backup and disaster recovery are two of the most commonly sought cloud-service scenarios, encompassing laptop/endpoint protection, file-sharing/collaboration, and offsite secondary repositories. For many, the easiest solution is simply to take advantage of the current backup software's or hardware's capability to replicate an additional copy of data to a cloud provider. Several ways exist to get to the cloud for data protection, and ESG expects it will continue to be a hot area of innovation for years to come.

Four Things That You Should Do NOW

"Right-sized" data protection is achievable in solutions that can meet the needs of organizations of any size with the reliability that you deserve and the simplicity/affordability that you require. Here are some next steps to consider:

1. Build awareness among your business stakeholders around the importance of better-than-mediocre data protection based on what the impact to the business would be after a realistic, non-optimistic assessment of your current capabilities. With that, drop any assumptions that midsized organizations can't afford anything more than a bare-bones solution. Instead, recognize that midsized organizations cannot afford downtime, lost data, or lost credibility with their customers or partners.
2. Continue or accelerate your virtualization journey because of the operational benefits that you'll immediately gain and the data protection agility that also comes from it, including whole-machine protection and portability during unplanned interruptions and planned migrations. And wherever you are in that journey, ensure that your virtualization protection capabilities include reliable protection using the hypervisors' APIs, application-aware protection and recovery options, and the ability to do granular recoveries (i.e., files from within a VM).
3. Modernize your data protection medium, including the consideration of both contemporary tape (LTO5 or LTO6) and deduplicated disk—either of which (or both) should yield new efficiencies in storage, as well as improved protection and recovery times. Start by testing your recovery speeds and assessing your backup windows; and you'll probably discover some areas the need improvement.
4. Get your data out of the building; either to a secondary, self-managed facility or to a cloud-based service. Even if you don't have a grandiose BC/DR strategy or toolkit, an additional copy of your data in a separate location can mean the difference between your business surviving or shutting down in the event of a crisis or outage.

The Bigger Truth

SMBs deserve enterprise-caliber data protection, but they can’t afford to go buy enterprise products with enterprise price tags and enterprise complexity. Even though your “data center” may fit in a closet or a small office, you don’t need to settle for inadequate protection. Because midmarket organizations depend on their data but don’t have a secret superhero waiting in the wings, they arguably need even better data protection. In other words, SMBs need enterprise-quality data protection, right-sized for them.

To be clear, most midsized organizations underestimate the level of protection that they need, similar to how many individuals underestimate long-term financial preparedness. That analogy continues with the recognition that by continuing to remain under-protected, midsized organizations risk catastrophes that could have been avoided by a few strategic changes.

The good news is that vendors of “traditionally enterprise” technologies are answering the call by right-sizing their hardware and redesigning and recreating the management/user experience in order to accommodate the IT pro generalist whom most midmarket organizations rely upon—with the result being data protection that is reliable, affordable, and easy to use.

HP Pub No. 4AA5-1360ENW