E-Guide

2015 Data Backup/Data Protection Planning Guide

A compilation of our best educational content from editors and experts, and industry statistics to prepare you for your DR planning
The package of information you just downloaded was written and assembled as an excellent guide for IT professionals, like yourself, who are looking to address disaster recovery planning. In a recent survey, we asked qualified IT professionals in Asia Pacific on their data backup/data protection purchases and plans for the coming months. 76% of respondents said they are purchasing new technology to help with their disaster recovery planning.

In this e-guide you will find related articles, including best practices and technical tips to help your organization with everything you need to know for DR planning.

We hope you enjoy this package of information and find it useful when developing your new data backup plan and strategies in your organization.
Which challenges is your organization looking to address with your new technology purchase?

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster recovery planning</td>
<td>76.04%</td>
</tr>
<tr>
<td>Server virtualization backup</td>
<td>58.95%</td>
</tr>
<tr>
<td>Backup operations consolidation</td>
<td>37.50%</td>
</tr>
<tr>
<td>Addressing growing data volume</td>
<td>34.38%</td>
</tr>
<tr>
<td>Compliance</td>
<td>34.38%</td>
</tr>
</tbody>
</table>

76% of our respondents are purchasing new technology to help with their DR planning.

10 mistakes to avoid in your disaster recovery planning process

Don’t make your DR planning process harder than it is by trying to do too much or cutting corners. Careful planning is key to a successful recovery.

At the start of the new year, many IT folks (and perhaps a few business managers) resolve to take steps to prevent avoidable interruption events and to cope with interruptions that simply can’t be avoided. In short, they decide to get serious about data protection and disaster recovery planning for business IT operations.

Why the disaster recovery planning process can be so tough

Disaster recovery (DR) planning is a complex and time-consuming task when done properly, which helps to explain why, for the past few years, surveys have shown the number of companies with continuity plans on the decline. In one annual PricewaterhouseCoopers study, companies with DR plans are down from roughly 50% of those previously surveyed to approximately 39%
last year. Of these companies, the ones that actually test their plans are usually a fraction of those that claim to have a plan, raising further concerns about the actual preparedness of those firms with documented, but untested, plans.

Planning activity has also dropped off because of misperceptions about its necessity and value. Intuitively obvious though it may seem that "doing more with less" means "doing more with computers," and that downsizing staff actually increases dependency on the uninterrupted operation of the automation resources and reduces tolerance to even a short-term interruption, the connection between these insights and the need to ensure that automation is resilient and continuous isn't being made.

Money is also a hurdle, as it always is. Managers can always think of ways to invest money so that it makes more money for the organization -- an option that's generally preferred to spending money on a continuity capability that may never need to be used. With some economic uncertainty in today's marketplace, this normal preference to focus spending on initiatives with revenue-producing potential is even more distorted, often at the expense of initiatives focused solely on risk prevention.

**DR is an investment**

Common sense regarding the need to allocate budget, resources and time to the DR planning process may also be diminished by the marketecture and hype around technologies such as server virtualization, data deduplication, clouds and so on.

Over the past few years, vendors have spent considerable effort trying to convince users that a side benefit of those technologies is improved or increased protection for data and operations. "High availability trumps disaster recovery," according to one server virtualization hypervisor vendor's brochure. "Tape Sucks. Move On" was emblazoned on bumper stickers distributed at trade shows by a dedupe appliance vendor. "Clouds deliver Tier 1 data protection," claimed a service provider's PowerPoint. These statements suggest that disaster recovery planning is old school, replaced by resiliency
and availability capabilities built into new products or services. However, most of these claims are downright false or, at least, only true with lots of caveats.

1. **Don't think high availability equals DR.** Perhaps the first and most important mistake to avoid when undertaking to build a disaster avoidance and recovery capability is to believe vendor hype about the irrelevancy of DR planning. While improvements might be made in high-availability (HA) technology, this changes nothing about the need for continuity planning. HA has always been part of the spectrum of alternatives for accomplishing a recovery from a disaster event. However, the use of HA strategies have always been constrained by budget: HA (failover between clustered components) tends to be much more expensive than alternatives, and is inappropriate for workloads and data that don't need to be made available continuously. For most companies, only about 10% of workloads actually fall into the "always on" category.

2. **Don't try to make all applications fit one DR approach.** A second common mistake in planning, and one closely related to the first mistake, is to try to apply a one-size-fits-all data protection strategy. For the same reason that failover clustering isn't appropriate for all workloads, all data doesn't require disk-to-disk replication over distance, disk-to-disk mirroring, continuous data replication via snapshots or some other method. The truth is that most data can be effectively backed up and restored from tape. Using disk for everything, including backup data, may seem less complex, but it tends to be far more costly and far less resilient. Given the numerous threats to disk storage, the problems with vendor hardware lock-ins for inter-array mirroring and replication, the costs of WANs and their susceptibility to latency and jitter, and many other factors, disk-to-disk data protection may not be sufficient to protect your irreplaceable information assets. At a minimum, tape will provide resiliency and portability that disk lacks. Think "defense in depth."

3. **Don't try to back up everything.** Expecting all your data protection needs to be included in a single backup process is another common mistake. The truth is that a lot of your data, perhaps as much as 40% to 70%, is a mix of archival-quality bits -- important but non-changing data that should be moved off production storage and into an archive platform -- and dreck (duplicate and
contraband data that should be eliminated from your repository altogether). Only approximately 30% of the storage you have today requires frequent backup or replication to capture day-to-day changes; the other 70% requires very infrequent backing up, if at all. You can take a lot of cost out of data protection and shave precious hours off recovery times if you segregate the archive data from the production data. Doing so will also reclaim space on your expensive production storage environment, bending the cost curve on annual storage capacity expansion and possibly saving enough money to pay for the entire data protection capability that you field.

4. **Don't overlook data that's not stored centrally.** This mistake is forgetting about outlying data repositories. Not all important data is centralized in an enterprise SAN or some complex of scale-out network-attached storage (NAS) boxes. Mission-critical data may exist in branch offices, desktop PCs, laptops, tablets and, increasingly, smartphones. Recent surveys by TechTarget's Storage Media Group reveal that even before the rise of the bring-your-own-device (BYOD) era, companies weren't doing a very good job of including branch offices or PC networks in their data protection processes. In another study published this year, 46% of 211 European companies admitted they had never backed up user client devices successfully and that BYOD looms on the horizon as a huge exposure to data loss. You need to rectify this gap and may find it possible to do so with a cloud backup service, provided you do your homework and select the right backup cloud.

5. **Don't mismanage data and infrastructure.** Another mistake DR planning newcomers often make is ignoring root causes of disaster, which are lack of management of data and infrastructure. Lack of data management, or rather the failure to classify data according to priority of restore (based on what business workflow the data supports), is a huge cost accelerator in the disaster recovery planning process. Absent knowledge of which data is important, all data needs to be protected with expensive techniques. As for infrastructure, you can't protect what you can't see. The failure to field any sort of infrastructure monitoring and reporting capability means that you can't respond proactively to burgeoning failure conditions in equipment or plumbing, inviting disaster. These gaps can be addressed by deploying data classification tools (and archiving) to manage data better, and resource management tools to
manage infrastructure better. And, with respect to infrastructure management, tell your equipment vendors that you will no longer be purchasing their gear if it can't be managed using the infrastructure management software you've selected. That will also have the effect of driving some cost out of your normal IT operations.

6. Don't try to duplicate equipment configurations at the recovery site.
No. 6 in our countdown of DR preparation mistakes is developing a plan that replaces full production equipment configurations in the recovery environment. Given that only a subset of applications and data typically need to be re-instantiated following a disruptive event, you don't need to design a recovery environment that matches your normal production environment on a one-for-one basis. Minimum equipment configurations (MECs) help reduce the cost of the DR environment and simplify testing. Often, there's also an opportunity to make use of server virtualization technology to host applications in the recovery environment that you may not entrust to a virtual server under normal circumstances. Testing is key to making the transition, whether from physical host to MEC host, or physical to virtual.

7. Don't forget to fortify your WAN connections.
Vesting too much confidence in WANs and underestimating the negative impact they can have on recovery timeframes is in the No. 7 slot on our list of DR planning process mistakes. WANs are services that must be properly sized and configured, and that must perform at peak efficiency to facilitate data restoration or to support remote access to applications either at a company-owned facility or in a cloud hosting environment. Regardless of the service-level agreement promised by your cloud host or cloud backup service provider, your actual experience depends on the WAN. Don't forget about providing redundancy (a supplemental WAN service supplied via an alternative point of presence) in case your primary WAN is taken out by the same disaster that claims your production environment. And also keep in mind that your WAN-connected remote recovery facility or backup data store should be at least 80 kilometers from your production site and data as a hedge against both sites being disabled by a disaster with a broad geographical footprint. Most metropolitan-area networks that provide lower cost, high-bandwidth multiprotocol label
switching (MPLS) connections do NOT provide sufficient separation to survive hurricanes, dirty bombs or other big footprint disasters.

8. Don’t put too much trust in a cloud provider. While not yet as prominent as some of the aforementioned potential pitfalls, our eighth mistake is placing too much trust in a cloud service provider to deliver disaster application hosting or post-disaster data restoration. If you’re using an online backup provider, for example, you’ve probably moved data to the backup cloud in a trickling fashion over time. You might be surprised how much data has amassed at the service provider, and the length of time and the amount of resources that would be required to transfer it back to a recovery environment. Remember: Moving 10 TB over a T1 network takes at least 400-odd days. Alternatively, if your plan is to operate applications at a cloud infrastructure provider, using the latter as a "hot site" for example, then be sure to visit the cloud provider’s facility in person. In the 1970s, when hot site facilities were first introduced, there was a guy selling subscriptions to a non-existent hot site who, once his scam was discovered, retired to a non-extradition country before he could be arrested. At a minimum, if you plan to use a cloud to host your recovery environment, make sure that it actually has all the bells and whistles listed in the brochure, including that Tier-1 data center.

9. Don’t let app designs foil DR. This mistake is procedural: planners need to stop accepting the notion that DR planning is a passive activity -- that you’re dealt some cards and are required to play the hand as it was dealt. For business continuity capabilities to be fully realized, resiliency and recoverability should be built into applications and infrastructure from the outset. However, few DR-savvy folks have been given seats at the tables where applications are designed and infrastructures are specified. This must change going forward. Put bluntly, bad design choices are being made right now that will obfuscate some company’s recovery efforts in the future, including the platforming of applications and data in proprietary server hypervisors or storage platforms, coding applications using insecure functions, employing so much caching that significant amounts of critical data will be lost if an interruption occurs and so on. If DR planners can get involved early on, better design choices can be made and IT can be made much more recoverable at a much lower cost.
10. Don't forget to follow the money. Management holds the purse strings, so it could be a big mistake if you don't make the case for your DR plan based on business value rather than technical terms. You need to show management that you're doing everything possible to drive cost out of the continuity capability without sacrificing plan efficacy. You also need to emphasize investment risk reduction and improved productivity enabled by the plan, thereby providing a full business value case. Only then will you have a chance of overcoming the natural reluctance of management to spend money on a capability that in the best of circumstances will never be used.

For the record, the greatest expense in DR planning isn't the cost for data protection, application re-instantiation or network re-routing; it's the long-tail cost of testing. So, try to build a capability that can be tested as part of day-to-day operations, alleviating the burden on formal test schedules, which should serve as logistical rehearsals (not tests) of whether data can be restored.

About the author:

Jon William Toigo is a 30-year IT veteran, CEO and managing principal of Toigo Partners International, and chairman of the Data Management Institute.

Tech Talk: Backup and disaster recovery plan best practices

Q&A with Jon Toigo, disaster recovery guru.

What aspect of backup and DR [disaster recovery] can be dealt with together without messing up either process?

Jon Toigo: They're integral processes. They're joined together at the hip. I would say that the nexus that maybe isn't really understood between backup and disaster recovery is that disaster recovery plans have to be tested periodically to make sure that they are going to work and to make sure they're still up to date with what's required to recover business processes, which is what it's all about. A lot of people waste a lot of precious time for testing, doing data recovery testing, seeing whether they can recover data successfully off of a set of backup tapes, or seeing whether data has been mirrored and we can switch to the mirrored copy of the data when the time comes.
We shouldn't have to do that as a part of disaster recovery testing. It increases the length of the test. It increases the costliness of the test. We should focus on a data protection scheme that gives us the ability to test the integrity of the data that we've captured, the right data that were copied, the right data that the data is restorable, that the data is recoverable. We should be able to do that on an ad hoc basis as part of the day-to-day operation. We shouldn't have to do that as part of a formal test.

So, I think the best thing is define a data protection strategy, like backup, that can be verified independently and test it on an ongoing basis, not as part of a formal test, which is a part of disaster recovery planning. But you keep trying to separate or differentiate backup from disaster recovery. The two are integrally related. There's no reason to do a backup unless it's for disaster recovery.

**Does where you put your data copies change the way you approach DR?**

Toigo: I would say, as long as you make a copy and store it off-site, you're about 99% of the way there. You want to do that across a WAN from one disk to another disk, that's an approach. It's an approach that some companies like to use. The trick is to make sure that the data is put far enough away from the original in terms of distance, because as you know, we just had Hurricane Sandy that came ashore in the Northeast.

We've had other disasters that had a very broad geographical footprint. And if the data copy is in the same zone of destruction as the original disaster, you're hosed, putting it simply. So you want to go at least 50 miles to 100 miles away with your copy. If you're doing that on a WAN, a wide area network, that's prohibitively expensive if there is a lot of data to move.

Moving 10 terabytes [TB] of data across a wire using OC192 technology available to core carrier network players, like AT&T, that'll take four hours. You do it across a T1 line, it will take over a year to move 10 TB of data. The fastest way ever invented to move data over distance is what's known as IPVAC -- IP, Internet Protocol over AV and carrier -- which is strapping a USB key to the leg of a passenger pigeon. The data gets there faster than it does going across a network. So, that's being kind of silly, but that shows some of the vicissitudes you run into with [WAN]-based disk-to-disk replication. Dubbing it to tape takes
advantage of that avian carrier, if you will, but the avian carrier might be FedEx.

Clouds are the worst of both worlds. First of all, we have to go across a wire to park it up in a cloud, just WAN-based replication. Also, if the cloud provider has a lot of an area that was devastated by, say, Hurricane Sandy, and they never once considered that everybody would ask for their data back at the same time. They didn't have the bandwidth to provide it, and we heard stories that some companies were waiting as long as a year to get their data back. Would you be able to go on with your business without your data for a year?

So, those are some of the gating factors on vetting these different solutions. Is it always the case? No. I mean, there are some clouds that have a little more alacrity than that, but then again, those clouds are probably within the same geographical areas as your company and both of you may get your clocks cleaned by a natural or man-made hazard with a broad geographical footprint.

So, you've got to be aware and plan to the worst-case scenario, and figure out [how] to do it in the most cost-effective way.

If a company is trying to look at data protection holistically, where should they start? Backup, DR or archiving?

Toigo: I would say that where you start for holistic data protection is how you create an infrastructure. I want to only have gear that's manageable -- in other words, that I can see. Unfortunately, a lot of us haven't deployed infrastructure that's manageable. Now there are a couple of ways we can do this.

We can design it in and ask all of [our] vendors to build in some capability into their gear like RESTful management, which is based on a standard called REST [representational state transfer] from the World Wide Web consortium. And we can wait for them to do that, which they may or may not ever do; or we can choose one of the management products that are out there, like Tivoli, CA, Symantec or whatever, and we deploy it and that's going to be our storage management framework for now on; and we tell every vendor we're not buying your gear unless you can be managed using this common management utility. Because we need to know what's going on with the infrastructure, because a disproportionate amount of data disasters accrued to failures of whatever type.
We want to see those situations burgeoning so that we can correct them before they hurt us. Now, beyond that is the data management problem. Data, when it's written by an application, an end user should be afforded a set of services [that are] appropriated to that data. If it's data we're going to hold on to for a long time, maybe it needs to become a part of [a] tiering scheme. The data gets first written to really fast storage, where it's used during the time when it's accessed a lot, and then it migrates to slower storage, with a greater capacity and lower costs, and then it migrates down to tape. If you do that in a rigorous way, you end up with about 60% of your data down at the tape layer, and that dramatically reduces the costs of your infrastructure. If you've got a 100 TB infrastructure, your total cost of ownership if you're using tiering like I described, is going to be $350,000 average. If you're not, if you're using just two tiers -- disk and disk, fast disk, slow disk -- it's going to be somewhere in the neighborhood of $150 million.

These numbers are coming from one of the gods in this industry, a guy who runs Horizon Information Strategies. His name is Fred Moore, and he did the definitive work on storage tiering and what it costs. Now, that's a service applying a policy for data migration over its useful life. Another set of services might protect against different kinds of data disasters -- I call that defense in depth. There's a possibility that data can become corrupt when it's written to disk. So, maybe you want to do something like RAID or erasure coding, or one of these other techniques like continuous data protection where you're writing the data somewhere else on a continuous basis, so if you write it to disk and the disk fails or the data is corrupted when it's written, you can recover the data that's local.

What happens if somebody drops a can of Coke inside the cage, and it spills down the backplane of your array and fries it? What happens if a sewer pipe in a ceiling breaks and you can't go into it because it stinks or because it's unhealthy, it's a biohazard. Believe me, I've been through all of this. I've seen all of these things.

Then you have the geographical-footprint disasters, the hurricanes, the earthquakes, the CNN-style stuff, a terrorist attack, all of that. You're going to need different modalities to protect the data against different possibilities. The
local one in the facility might be a mirroring scheme where it replicates data on an ongoing basis from an array over here to an array over here sitting right next to it or somewhere else on the corporate campus. It's all internal to the LAN of the company. Whereas the geographical disaster may require tape backup with off-site storage, may require WAN-based replication, something like that.

So, chances are you're going to be using an interlocking set of data protection strategies, all integrated as a set of services; and I should ideally be able to check mark as I write data, say, this data is going to get this service, this service and this service, and send it to that volume. I can do that if I virtualize my storage infrastructure. I can define virtual volumes to write data that offers different combinations of services.

**What do you think the most frequent mistake is for companies trying to put together backup and DR plans?**

Toigo: Two things: One, they tend to get too preoccupied with the threats. So, they end up writing a great script for a sci-fi movie. They spend a lot of time developing scenarios, because that's fun to do too. I used to do that too. It's better for a Hollywood screenwriter than for a DR planner: You spend an exorbitant amount of time creating, 'Well, okay, terrorists break in, and they blow this up, and they cut these wires; and you know, how are we going to protect from something like that?'

Well, you know, you hire Bruce Willis. We all know that. Or an asteroid is coming from outer space, and how are we going to protect our facility and our data against that? Who cares? It's game-over at that point. Let's figure out the reality. So, I say, just assume you got a worst-case disaster and then build a plan in a modular way so that you can respond to any kind of an emergency that might come along -- that's the practical method. The second thing you do is to make sure that whatever you choose to deploy as a strategy for data protection, for disaster recovery, that it can be tested.

I want to make sure I've got a dashboard that shows me that a mirror is working, because mirrors themselves are inherently non-testable. You have to quiesce the application, flush the data out of the cache, write it to disk one and
mirror it to disk two, shut the whole thing down, and then do a file-by-file comparison between disk one and disk two to make sure you're copying the right kind of data. That takes a long time. Nobody ever does that. It's a hassle. So, we're exposed.

What we want to do is find a way to do that where we can test things readily.

Last, don't call it disaster recovery. Management has this knee-jerk reaction not to want to spend money on protecting against a possibility that may never happen.

So, anyway, a lot of people tend to become so preoccupied about the threats that are associated with a disaster, they frame everything in, 'Oh well, we need to act immediately to safeguard against these disasters.' Management doesn't get that. So, what you need to do is call it something else. Lie, call it something completely different. Say, 'We're putting together data compliance. We're making sure the data we have to hold onto under HIPAA for the next seven to 10 years will be properly kept safe so that we're in compliance with the regulation and you won't go to jail.' If you call it something else -- compliance management, whatever -- you're likely to get funded, but if you call it disaster recovery, in my experience, nobody is going to give you any money for it.

About the author:
Jon William Toigo is a 30-year IT veteran, CEO and managing principal of Toigo Partners International, and chairman of the Data Management Institute.
What are the most important factors for your organization when evaluating and purchasing data backup and recovery technologies?

58% of our respondents said that capacity was their most important consideration

Partners weigh discovery, capacity planning tool choices

Sizing up your customers' complex IT environments today often demands you use sophisticated tools instead of guesswork. Partners weigh in on an array of tools for discovery and capacity planning and discuss which one works best for them.

Channel companies are employing a mix of free and price-marked tools to size up their customers' increasingly complicated IT environments.

In past years, experience, rules of thumb and comparisons with customers of similar size may have been enough for solutions providers to determine the proper configuration. But customers' complex server, storage and networking deployments make the seat-of-the-pants approach somewhat risky. Organizations run a mix of physical servers and virtual machines and operate
multiple tiers of storage with different capacity and performance characteristics. Resellers and integrators need to deal with more variables. A range of tools and utilities, however, automate the task of discovering the devices that are tethered to customers’ networks. Such tools collect utilization and performance data and then report the numbers for guidance in capacity planning.

Tools come from a couple of sources and provide various degrees of infrastructure coverage. Storage vendors, for example, sometimes offer their channel partners free discovery and capacity planning tools. Software companies -- ranging from major players such as Microsoft and VMware to smaller, more specialized companies -- also offer utilities. Solutions providers may need to use more than one tool to get the job done, especially when they go beyond servers and storage to explore desktops and mobile devices.

While discovery, planning and configuration tools have existed in various forms for some time, the latest crop of tools surpasses the earlier technology.

"Tools have become very sophisticated these days," said Joe Brown, president of Accelera Solutions, a Fairfax, Virginia-based solutions provider that focuses on the cloud and virtualization. "They are much easier to operate than they used to be."

A range of tools
As a virtualization specialist, Accelera leverages much of its tooling from VMware. For example, the company uses VMware's vCenter Operations Manager, which, according to VMware, probes the performance, capacity and health of an organization's IT infrastructure.

The vCenter Operations Manager utility, sometimes referred to as "vCOps," can be purchased as part of VMware's vCenter Operations Management Suite. But VMware offers the Foundation version of vCOps for free with every edition of vSphere, the company's server virtualization platform.

Brown said his company uses vCOps as its primary tool in server environments for such tasks as evaluating resource consumption and planning
for future capacity requirements. He said the VMware tool lets the company evaluate a customer's current hardware environment and workload, and then determine the central processing unit (CPU) resources and I/O Operations Per Second (IOPS) necessary to support the same workload in a virtual environment.

While Accelera uses VMware tools for capacity planning on the server side, the company uses Lanamark Inc.'s Lanamark Suite for a more comprehensive view that takes into account desktops as well as servers, Brown explained. Lanamark Suite discovers customers' physical and virtual infrastructure and supports desktop virtualization and cloud migration planning.

Brown said Lanamark helps Accelera determine what it would take to transition a customer from its current computing model to a cloud-based approach.

"This tool will walk you through the process of modeling what ... the target cloud environment would look like," he said.

Outside of virtualized environments, Accelera uses tools associated with Microsoft System Center, which is used for managing Windows Server networks.

**A one-tool focus**

Other companies focus mainly on one discovery and capacity planning tool. Advanced Computer & Network Corporation (AC&NC), a storage solutions provider based in Pittsburgh, works with the American Megatrends Inc. (AMI) StorTrends product line and the StorTrends iDATA utility. The iDATA tool is a component of the AMI StorTrends Profit Program, a channel initiative launched in June.

Gene Leyzarovich, president of AC&NC, a StorTrends channel partner, said iDATA gauges customers' storage performance, latency and network utilization among other attributes.
"It gives us a snapshot of what they have and how we can size the storage equipment for them," he said, noting that the company has been using the utility for about four months.

Using the free-of-charge iDATA, AC&NC can look at network utilization to determine whether the customer needs gigabit Ethernet or 10-gigabit Ethernet technology. Leyzarovich said the tool also tracks IOPS usage, which he said helps determine storage requirements for virtual desktop infrastructure (VDI) projects.

Leyzarovich said iDATA provides the features the company needs to size the customer's environment and propose the appropriate storage gear. He said other tools, by comparison, may just provide network monitoring or I/O monitoring. Another benefit: iDATA serves as a sales tool that the company can lead with when approaching prospective customers.

"It helps us to eliminate a lot of the back-and-forth with the customer," Leyzarovich said.

Previously, the company would ask a long list of questions over several phone calls to get a sense of the customer's IT environment and requirements. The iDATA tool, however, provides the data without the need for multiple consultations.

"It gives you a full picture right away," Leyzarovich said. "It probably saves five to 10 phone calls."

The launch of AMI StorTrends' 3500i product, solid-state drive (SSD) hybrid or full-flash storage-area network (SAN) array, prompted the company to create iDATA. AMI StorTrends rolled out a pre-production beta of the 3500i last October and soon found that customers were clamoring for a tool to size their SSD capacity requirements.

A customer may seek to replace a number of traditional spinning disks, which could include a mix of 7,200 RPM, 10,000 RPM and 15,000 RPM Serial-Attached SCSI products, Justin Bagby, director of AMI's StorTrends division,
explained. Without a tool, attempting to translate such an environment into SSD capacity and IOPS would amount to guessing, he added.

As a basic input/output system manufacturer, AMI has an in-house utilities development group, which created iDATA. The tool was released in beta mode in January and went into production in April. The utility supports Windows, but a Linux version is in beta and slated for production in about a month, Bagby said.

The iDATA tool lets a partner select a customer’s networks and discover the attached servers. The tool creates a list of the servers and also identifies all the disks on a server or every data store on a VMware ESX host. The partner selects which servers and storage equipment to monitor and chooses how many days to conduct the monitoring, from one to seven.

The iDATA utility collects data on such measurements as IOPS, throughput, read/write ratio, peak disk latency, peak queue depth for direct-attached storage and SAN, CPU utilization, and memory utilization. The tool also shows capacity growth over the monitored time span and extrapolates that number over a 12-month period. The tool generates a report file at the end of a monitoring run.

**Tool limitations**

Automated tools take the guesswork out of sizing storage and server configurations, but they face some limitations. For one, channel partners need to be mindful of the day and time that the tools run. Leyzarovich pointed to the example of a customer assessment conducted during a holiday week that came up with 6,000 IOPS, while 10,000 IOPS was a typical reading for peak hours during the customer’s normal business week.

Brown, meanwhile, suggested that tools for analyzing the mobile environment could use some work. Mobile tools require partners to install a software agent on each monitored device, which Brown said can prove cumbersome in some cases. And tools lack cross-platform support, which forces solutions providers to collect data from a number of different utilities and then attempt to rationalize the data, he added.
Another difficulty is not the fault of the tools, but rather a consequence of their ability to extract data from customers' IT deployments. Brown said the top challenge isn't collecting information, but how to use it for the customer's benefit.

"We certainly we have more than enough data," Brown said. "It is more about how you analyze the data and what the best scenarios are for the customers."

About the author:
John Moore has written on business and technology topics for more than 25 years.

New storage capacity management tools can make efficiency a reality
Poor provisioning and a lack of effective capacity management tools leads to underused storage systems. New tools and improved processes can make storage efficiency a reality.

Storage managers rarely admit they have a capacity management problem. Instead, they're more likely to talk about how big a slice of their IT budget storage eats up or the unpleasantness of unplanned purchase requests. In some cases, the conversation focuses on the high cost per gigabyte of storage.

Other managers may be preoccupied with seeking a solution to seemingly unattainable backup windows or impossible disaster recovery scenarios. Some are looking for capacity management tools or processes that can identify and prune obsolete data, while others are buying storage in large chunks annually to get "quantity discounts."

What do all of these scenarios have in common? In each case, storage managers are trying to address a symptom without taking a holistic view of a fundamental problem: the lack of an effective storage capacity management regime.
Don't look to the cloud for answers

Let's state up front that cloud storage is not the solution to a capacity management problem. Increasingly, cloud is portrayed as the cure-all for what storage ailments are afflicting companies. Cloud may mask the pain with a somewhat lower cost per GB, but it does nothing to fundamentally address uncontrolled capacity expansion. Cloud has a role in storage service delivery, but solving capacity problems isn't one of them.

It would be charitable to say that some organizations' storage utilization is less than stellar. Many companies have as little as 20% to 30% average utilization as measured by storage actually consumed. Those organizations whose consumed utilization is more than 50% are the exception. This metric is one of the fundamental obstacles to better utilization.

There are three basic ways to measure storage capacity:
- **Formatted** (sometimes referred to as raw, though there is a technical difference)
- **Allocated** (sometime expressed as provisioned)
- **Consumed** (or written)

When asked what their utilization rate is, most storage administrators will quote the allocated figure. From their perspective, if it's allocated to an application, it's as good as consumed because it's unavailable for new provisioning. It's a legitimate perspective, but it can cover an insidious incentive to overprovision because it allows that portion of storage to be ignored for a long period of time. Some administrators will tout an 85% utilization rate, even though perhaps only 20% of the array has actually been consumed. Such poor utilization, however, ultimately drives up the average cost per GB consumed by 2x or more with management none the wiser. Moreover, most capacity purchases are triggered when allocated capacity hits 85% regardless of how much is really being consumed. Responsible teams husband an organization's resources more diligently.

Why is data getting so big?

The biggest driver of storage growth is "secondary" data, copies of original data or primary storage. Secondary data includes snapshots, mirrors,
replication and even data warehouses. The secondary data multiplier can be as high as 15:1. It would seem the obvious solution is to reduce the number of data copies, which may indeed be the case. However, the secondary copies were likely created for a reason, such as for data protection or to reduce contention for specific sets of data. The unintended consequence of optimizing storage capacity management may be reduced data recovery capabilities or worse performance. Thus, storage managers must be aware that there's an inverse relationship between data recovery, performance and capacity management; if you improve one, you're likely to impede the other. Consequently, it's important to start with service-level requirements for recovery and performance. Capacity management can be optimized only to the point that other service levels aren't jeopardized.

**Tools to take control of capacity management**

**Thin provisioning**
- Eliminates overallocation and increases utilized capacity from 30% to 60%
- Cuts the cost per gigabyte (GB) stored by 50%

**Compression**
- A 2:1 compression allows twice as much data in the same array, for another 50% reduction in cost per GB stored

**Deduplication**
- A 2:1 deduplication rate further halves the cost per GB of storage and the deduplication rate could be higher for some data types

**Storage resource management applications**
- Manages storage as an enterprise, not as individual arrays
- Measures storage metrics to drive best practices
- Spots trends that could become serious problems without proper attention

**Capacity management toolkits**
Fortunately, storage managers have numerous tools to assist them in tackling capacity management. These include two general categories: utilities and reporting tools. Array vendors have a number of useful utilities that are now available with most systems.
Perhaps the most common of these is thin provisioning capability, which is supported by nearly every vendor. Thin provisioning allows administrators to logically allocate storage, but automatically keeps the physical allocation only slightly above the actual capacity used. Storage is automatically allocated from a common pool as a volume demands more space. Because the array itself may be logically overallocated, it’s possible to have an out-of-space train wreck if administrators don’t ensure that enough physical capacity is available as data grows. This is uncommon, however, as automated alerts should keep administrators on top of the situation. Thin provisioning alone can largely alleviate the problem of high allocation/low utilization. In most cases it’s complemented by a space reclamation feature that returns unused space to the common pool. While array vendors may offer this feature, reclamation can also be performed by Symantec Corp.’s Veritas Foundation Suite for those who use that product.

Another useful and near-universal utility is compression. Most vendors are willing to guarantee a 2:1 compression on primary storage, or a 50% space savings. Compression is normally applied at the LUN or volume level, depending upon the vendor’s specific implementation. Compression does incur some performance penalty, though it can be as little as 5%. Of course, your mileage may vary, so a proof of concept is worth the effort. From a management standpoint, the benefit of compression is cutting the cost per GB stored by 50%.

Compression is complemented by data deduplication, though deduplication is not yet supported on primary storage by every vendor; EMC Corp. and NetApp Inc. are examples of vendors that do. Here again, deduplication differs in its implementation on primary storage versus backup appliances. On primary storage, data deduplication is an idle-time process and isn't nearly as aggressive in eliminating duplicate blocks as deduping backup appliances. Because it’s a background process, the compression itself doesn't impact operations. Decompression, known as "rehydration," may have minimal or significant effect on performance, so a proof of concept is advised. Rehydration is more like reassembly of parts. Unlike compression where vendors make efficiency guarantees, there are no such guarantees with
Capacity management reporting tools

The other category of tools is reporting tools, or more accurately, storage resource management (SRM) products. Both array vendors and independent vendors offer SRM products, examples of which include EMC ControlCenter, Hewlett-Packard (HP) Co.’s HP Storage Essentials, NetApp OnCommand Insight (formerly SANscreen) and Symantec’s Veritas CommandCentral Storage. All of them offer the ability to comprehensively manage and monitor an enterprise storage environment. Yet few organizations leverage them, largely because SRM has gained a reputation as being unwieldy and resource-intensive. These limitations can be overcome by focusing on only those aspects of an SRM application that are truly beneficial, otherwise known as the 80/20 rule. In the context of storage capacity management, you should focus on the following:

- **Thresholds.** Individual arrays provide threshold alerts, but SRM applications can consolidate them and give an enterprise-wide picture to administrators. This allows far more comprehensive planning and provisioning to prevent one array from being oversubscribed while another is undersubscribed, for example.

- **Utilization.** Again, SRM consolidates information that otherwise must be manually aggregated (and who has the time to do that?). Utilization figures to monitor include:
  - **Consumed as a percent of raw.** Know how much the array is truly utilized. Target 55% or higher as a best practice, though this will vary with the age of the array and growth rates.
  - **Consumed as a percent of allocated.** Know whether or not the array is overallocated. Target greater than 70% (85% if thin provisioning is used) as a best practice. Allocations lower than 70% may be acceptable for newly provisioned LUNs or those with high, unpredictable growth.
  - **Secondary data.** Know how much data is consumed by snapshots, mirrors and the like. Target no more than 3x the deduplication because it's highly dependent upon data type. Media files generally dedupe poorly, whereas text files may dedupe quite well.
primary storage. More than 3x may be justifiable for various reasons, but this ensures that space isn't consumed unnecessarily. This feeds into data/information lifecycle management.

- **Trends.** Thresholds and utilization are points-in-time. Identifying trends is the key to optimizing capacity.
  - **Growth rates.** Knowing growth rates fosters accurate forecasting, thereby avoiding unnecessary "safety factor" purchases. Storage prices decline approximately 10% per quarter on a per-GB basis, so delaying an organization's purchases can yield substantial savings over time.
  - **"Days storage in inventory."** Using growth rates, calculate how many days of storage growth capacity is on the floor. Target 90 to 180 days. Less than 90 days doesn't give purchasing enough time to do their job most effectively. More than 180 days and you could have purchased the storage later at a cheaper price.

Organizations can dramatically cut the cost per gigabyte stored by using the array utilities that in many cases are already paid for. Implementing thin provisioning, compression and deduplication (where applicable) can reduce this cost by 50% to 75%, which isn't bad by any measure. However, best-organizations will implement SRM products to take their storage management to the next level. With it, storage managers can balance and optimize performance, data protection and capacity utilization simultaneously.

**About the author**

*Phil Goodwin is a storage consultant and freelance writer.*

If you are looking for more related tips and expert advice check out these resource pages on Disaster Recovery planning:

- [SearchDisasterRecovery.com](http://SearchDisasterRecovery.com)
- [SearchStorage.com](http://SearchStorage.com)
- [SearchDataBackup.com](http://SearchDataBackup.com)
Free resources for technology professionals
TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web’s largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?
TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

[Related TechTarget Websites]