

Realtime
publishers

The Essentials Series

Strategies for
Cloud Storage,
Data Protection, and
Disaster Recovery

sponsored by



by Don Jones

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We’ve made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book’s production expenses for the benefit of our readers.

Although we’ve always offered our publications to you for free, don’t think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you \$40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the “realtime” aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We’re an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I’m proud that we’ve produced so many quality books over the past years.

I want to extend an invitation to visit us at <http://nexus.realtimepublishers.com>, especially if you’ve received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you’re sure to find something that’s of interest to you—and it won’t cost you a thing. We hope you’ll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Introduction to Realtime Publishers.....	i
Article 1: What Can Cloud Storage Really Do For You?.....	1
Three Business Needs Your Current Storage Plan Doesn't Meet.....	1
Backup Windows	1
Time-to-Recover	2
Storage Utilization.....	2
Business Drivers for Storage, Data Protection, and Disaster Recovery.....	2
Data Accessibility.....	2
Downtime <i>Really Does Cost</i>	3
Be Strategic, Not Reactionary.....	3
Planning for Cloud Storage.....	3
Identifying and Sizing Critical Data	3
Identifying the Cost and Probability of Downtime.....	4
Fitting the Cloud Into Your Infrastructure	4
Optimizing Bandwidth and Storage.....	4
Rethinking Disaster Recovery.....	5
Cloud Storage: Pure Strategy for Storage and Data Protection.....	5
Article 2: Challenges and Special Considerations for Cloud Storage	6
Rules, Regulations, and Restrictions	6
Data Security Requirements	6
Data Location Requirements	6
Offsite Requirements	6
Recovery Objectives	6
What Are Your Data Categories?.....	7
How Much Downtime Can You Tolerate?.....	7
What Systems Need Protection?	7
Backups Alone Do Not Equal "Disaster Recovery Plan"	7

On-Site Recovery.....	8
Warm-Site Recovery.....	8
The Vendor Connection	9
Here’s Your New Storage Plan	10
Article 3: Leveraging the Cloud for Storage and Disaster Recovery: Three Practical Strategies.....	11
Keep Everything in the Cloud.....	11
Use the Cloud as a Backup	11
Hybrid Approaches.....	12
Onsite-Prime	12
Cloud-Prime	12
Other Hybrid Approaches.....	12
Hybrid Details	13
Conclusion	13

Copyright Statement

© 2010 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This book was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology books from Realtime Publishers can be found at <http://nexus.realtimepublishers.com>.]

Article 1: What Can Cloud Storage Really Do For You?

How long would it take you to recover your company's most critical data from your most recent backup tapes? Surprisingly, many companies don't know—and if they did, they'd probably be troubled. We've conditioned ourselves to accept the limitations of old-fashioned backup schemes and technologies, without realizing that better techniques have come along that better meet our business needs. The advent of cloud computing, and particularly cloud storage, now offers us the ability to create a *hybrid IT* model that really solves our business needs—and gets us back online faster in the event of a disaster. In fact, this new model of cloud storage can help address some of the problems with our entire storage plan—not just backup and recovery.

Three Business Needs Your Current Storage Plan Doesn't Meet

Ask most companies what their backup plan involves, and they'll probably say, "Backup tapes." Magnetic tape has been the primary medium for backups since the 1970s. Some companies store their backup tapes on-site, while others will smile knowingly and say that *they* send their tapes off-site for safekeeping. Nobody realizes, however, that those tapes aren't meeting their business needs.

The same thing applies to our storage plans in general: Just dumping everything on a file server in the office doesn't actually meet all of our business needs. We need to really examine those business needs, and look for ways to meet them, going beyond what we've done with storage for so many years.

Backup Windows

Tape backups usually consist of a snapshot of your data, taken during some kind of backup or maintenance window—usually at night. Any data that's changed or been created since the last tape backup is always at risk until the next backup is made—meaning we're potentially going to lose a day or more of critical data if a problem occurs.

This limited-time backup windows place restrictions on what we can back up, too: We can only protect as much data as we can cram onto a tape (or set of tapes) during the backup window's duration. We're constantly longing for faster tape drives, bigger tape cartridges, and faster transfer times so that we can grab more data during that precious window.

Cloud storage proposes to change the way you create and use backups by storing your data in highly-protected data centers *outside* your own facility—meaning your data is always safely backed up off-site, without any effort on your part.

Time-to-Recover

When we actually need to use those tape backups, we're left to sit and wait while data slowly streams off tape—while our business is losing money because we *need* that data. This is actually the biggest problem with old-fashioned backup techniques and storage plans: Tapes make for a safe, easy-to-carry form of backup, but they take *forever* to actually use when you need to recover data.

With cloud storage, there is much less time required to recover. Cloud storage vendors build highly-available, highly-redundant storage vaults so that your data is simply there when you need it, all the time.

Storage Utilization

How well do you actually utilize all that storage you've paid for—and that you pay to protect? Having a lot of extra storage lying around is like having an empty room in your house—it begs to be filled, and once you do, you'll have to manage it. Many companies place tight restrictions on what kind of data goes onto their storage, because they know they'll have to back it up—within that limited backup window. Restrictions mean that your storage isn't doing everything for you that it could, simply because you feel constrained to only store what you know you can protect.

Cloud storage helps to remove those constraints. You won't run out of backup storage, and you'll feel better about actually utilizing your storage because you know it'll be protected.

Business Drivers for Storage, Data Protection, and Disaster Recovery

No backup storage limitations. Faster recovery. Less infrastructure to maintain. Better storage utilization. Those are some of the main business needs that drive businesses to reconsider their storage plans, but there are other drivers, too.

Data Accessibility

Today's businesses don't run entirely out of the office. Employees work from home and on the road. In the event of a disaster, the entire company might need to pick up and relocate. Your storage plan should allow your data to be available anytime you need it, *wherever* you need it, without complex and expensive remote-access schemes. Your data should be safe, secure, private, and protected—but available in an instant from anywhere on the globe, if you need it.

Think about it: Being able to access your data from anywhere can solve a major problem that smaller companies have with disaster recovery: The need to plan for a disaster that involves your entire office or data center. Off-site recovery facilities are often expensive, and you're down for hours or days while you restore your data to the facility's servers. But if you could make your critical data available from anywhere, any time, then *anyplace* could become your off-site recovery facility. That's what cloud storage can offer.

Downtime Really Does Cost

Don't underestimate how much money you're losing while you're waiting for your data to be recovered from old-fashioned backup tapes. In business, time really is money, and when employees are waiting for data to be restored, you're not only wasting their time—and your money—you're also missing business opportunities, losing customers, and failing to succeed.

We've long *accepted* the fact that restoring data takes a long time because in the past that was simply the best we could do. But this isn't the past, and we don't have to automatically accept anything less than instantaneous access to our data. Cloud-based storage can offer that instantaneous access.

Be Strategic, Not Reactionary

The time to prevent your storage and data protection plan from being a failure is *before* a disaster occurs. You can't come up with a better storage plan in the face of a crisis; you have to pull some time out of your busy schedule *now*, and be strategic about your company's storage needs and data protection capabilities. You need to understand your business needs and evaluate new technologies—like cloud storage—and understand how they can help you craft a storage and data protection plan that really meets those business needs.

Planning for Cloud Storage

Cloud storage proposes that you store your data—at least some of it—in someone else's data centers. You might be storing a backup copy there, or you might be storing your actual live data there—it depends on your precise business needs. Once it's in the cloud, protecting your data is no longer your problem; it's your storage vendor's problem. Your data is simply available to you, all the time, without waiting, from anywhere with an Internet connection. The trick is in properly planning to utilize cloud storage as part of your total storage and data protection plan.

Identifying and Sizing Critical Data

It's probably reasonable to assume that not all your data is mission critical, and not all of it is in need of enhanced protection and faster—or instant—recovery in the event of loss or disaster. Cloud storage vendors commonly charge for the storage you use, so you'll want to begin by identifying the data that you want to protect in the cloud. Once you've identified your critical data, figure out how big it is. That will help you figure out how much cloud-based storage you'll need.

Identifying the Cost and Probability of Downtime

Cloud storage isn't free, of course—at least, not the kind of protected, secure cloud storage that you'll need. In order to weigh the costs and benefits, you'll need to have some idea of how much downtime actually costs you. Imagine that all the critical data you identified is suddenly gone, and your only hope for getting it back is that set of backup tapes in the trunk of your IT administrator's car. While you're waiting to see if those backup tapes really work, how much money are you losing? You also need to judge how likely it is for this situation to occur. How easily can data be lost? It doesn't have to be a meteor strike on your office; disasters can happen with the click of a "Delete" button by an incautious user.

Fitting the Cloud Into Your Infrastructure

So how does cloud storage fit into your current storage plan? There are actually several approaches and variations, which you'll learn more about in the third article in this series. Briefly, though, you can choose to:

- Keep all of your data in the cloud, and access it directly from there. This option provides great protection but requires solid, reliable connectivity to the cloud so that you'll be able to get to your data.
- Use the cloud for backups. Rather than backing up to tape, back up to the cloud. This method ensures that your backed-up data is available for instant use when you need it, but keeps your "live" data locally where it's easy to get to even if your Internet connection is down.
- Create a hybrid storage plan. There are numerous variations to consider, some of which include keeping your "live" data in the cloud and a "backup" copy locally in case your Internet connection fails. You may also choose to treat different categories of data differently, keeping the most critical data live in the cloud, where it's protected.

Optimizing Bandwidth and Storage

How will you get all your data into the cloud in the first place—and what's it going to cost to store it there? There are a few techniques and technologies that can help. *Compression* and *de-duplication* go a long way toward reducing the bandwidth needed to upload your data to the cloud and keep it up to date; some vendors claim up to an 80% reduction in data size through a combination of compression and the elimination of duplicate data segments. *Bandwidth throttling* helps ensure that your Internet connection isn't taken over completely by data uploads to the cloud, reserving as much bandwidth as you need for your production needs. And, once the data is in the cloud, compression and de-duplication help reduce its size—reducing the storage costs for you.

Rethinking Disaster Recovery

Storing your data in the cloud opens up fantastic new techniques for disaster recovery. Lose a server? No problem—your data is already in the cloud, and can be used to spin up a virtual machine in the cloud, too, duplicating your server’s functionality until you can get a replacement running. A disaster takes your entire office out of commission? Again, no problem: With your data in the cloud, all your critical servers can be brought online as virtual machines, and made accessible to your employees working at one or more alternative locations. This model is called a “warm site” recovery, meaning your recovery site—which is in the cloud—has copies of your data ready to go the minute you need them. Compare that to a “cold site” model, where you basically have to show up with your old-school backup tapes and start restoring them, and you’ll realize how much faster and more efficient the cloud-based model can be.

A good cloud storage vendor will help you get your own servers back online more easily, too. You shouldn’t have to pull an entire server’s worth of files and data down over your Internet connection; the vendor should be able to ship you tapes, optical media, hard drives, or other bulk-storage media so that you can get your servers up and running more quickly. Combined with “warm site” recovery models, you’ll get minimal downtime, and the ability to get your own data center back online as quickly as possible.

Cloud Storage: Pure Strategy for Storage and Data Protection

Cloud storage models offer significant advantages over the old-school backup techniques we’ve been using for years. In the next article, we’ll explore some of the specific considerations and special challenges that cloud storage needs to address, and consider some of the vendors that are making this space a reality. In the final article of this series, we’ll look specifically at practical strategies for cloud-based storage and disaster recovery, including specific models and some of their pros and cons.

Article 2: Challenges and Special Considerations for Cloud Storage

You're contemplating handing over at least some of your business' data to another company. What do you need to have in mind before you do so?

Rules, Regulations, and Restrictions

Start by considering any rules that may apply to your data. These rules may be particular to your industry, imposed by legislation, or might be the result of internal policies and business drivers.

Data Security Requirements

How secure does your data need to be, and how secure can a cloud storage vendor make it? Consider not only the encryption that the vendor uses in their storage centers, but also the encryption that protects your data while it's in transit to or from the cloud.

If you are subject to auditing rules—especially common for legislative compliance scenarios—how will the vendor ensure that you can continue to meet those rules? Can the vendor produce auditing reports that meet your particular compliance scenarios and provide the evidence that auditors require to prove that your data has been safe and secure?

Data Location Requirements

Are you permitted to move your data outside of your local jurisdiction? In some countries and industries, data has to be kept in-jurisdiction; you need to ensure that you're working with a cloud storage vendor who can meet that requirement.

Offsite Requirements

Are you *required* to move some data off-site for protection? If so, cloud storage can offer a faster, more convenient, and more automated way to make that happen. Be sure you understand what "off-site" means, too: Does that mean out of your office? Out of the city? Out of the region entirely, to guard against a regional natural disaster? Be sure your cloud storage vendor understands these requirements and can help you meet them.

Recovery Objectives

It's impractical for most businesses to provide the exact same level of protection for all their data, and in most cases it isn't necessary. You'll need to carefully define key recovery objectives so that you can begin identifying potential solutions and vendors that meet those capabilities.

What Are Your Data Categories?

Not all data is created equal. Some data is absolutely essential to your business. You may well want to store copies of that data locally as well as in the cloud for maximum access and protection. Other data is important, but less so; you may simply store copies in the cloud and accept the fact that accessing those copies over your Internet connection, should the need arise, might be slower. Some data may be so essential that you don't even keep copies locally: You store it entirely in the cloud, where it is continually protected and never at risk.

How Much Downtime Can You Tolerate?

Speed costs, so you'll need to determine how much downtime you can handle for each of your data categories. One reason to keep "live" data in the cloud, as opposed to merely keeping backups there, is to ensure the continual availability of that data—meaning you can't tolerate any downtime. For other data, you may be satisfied keeping the data locally and backing it up to the cloud, knowing that restoring the data may take a few hours if the need arises.

What Systems Need Protection?

Are you a completely homogeneous IT shop, or do you have a mix of operating systems (OSs) running your server and client computers? Ideally, you'll want a solution that can handle *all* your systems so that your storage can be centrally managed in one place. The ability to support multiple platforms is one area where cloud storage vendors truly differentiate themselves.

Backups Alone Do Not Equal "Disaster Recovery Plan"

You can't simply have backup tapes—or even cloud-based backups—and call that a "disaster recovery plan." An actual plan includes details on what you'll do in the event of a disaster so that there's no guesswork or mistakes—just consistent, rapid, thought-out responses.

There are really two broad models for recovering from a complete disaster: In the first, you assume that your data center is still operational and usable, and that you need to recover one or more specific servers. In the second, either your data center is unusable or unavailable, or the server you need to recover has had a complete hardware failure and can't be used.

On-Site Recovery

In an on-site recovery, your data center and server hardware is functioning, and you simply need to recover one or more servers. Using a cloud-based data protection plan, you have three options:

- Pull the needed data from the cloud. This can be time-consuming for a large amount of data, especially if you have a lower-bandwidth connection to the Internet.
- Have data shipped to you from the cloud provider. This can often be quicker than trying to copy all that data over the wire. A good vendor will provide different forms of media they can send you, and will offer rush or courier delivery services.
- Use a local copy of the data. This is obviously the fastest route, as the data you need is right within your reach. It does, however, require you to have *planned* for this scenario because you'll need to include a local copy of your data in your storage plan.

For example, suppose that a critical server fails. Because of its importance to your company, you've pushed all of its data into your cloud-based storage. You don't have a local copy of the data, so you decide to begin restoring the server by copying the data from the cloud. Your data is still available to users from its location in the cloud, so you don't have to wait until the server is back online to continue working. Downtime: Zero, or close to it. Even if an entire server failed, you would have minimal downtime if your cloud storage provider was able to restore the server to a virtual environment for you.

The last option in the previous list is a *hybrid* storage solution, something I'll cover in more detail in the next article in this series. The idea is that you keep a local copy of your data for speedier recovery capabilities, but also replicate that same data to the cloud—in lieu of tape backups and off-site tape storage—to ensure the protection of that data in the event of a larger disaster.

Warm-Site Recovery

If a critical server fails completely, or your entire data center is offline, what will you do? With cloud-based data protection, you can immediately start accessing your data—but what about servers that were running applications? It isn't enough, in other words, to have access to your database files—you also need a database *server*. This is where a good cloud vendor and a “warm-site” recovery model can come in handy. Simply ensure that your critical servers are *completely* backed up to the cloud, and the cloud vendor can launch virtual machines and restore your servers to those virtual machines, and your data *and* applications are up and running again. By creating a Virtual Private Network (VPN) connection between your network and the cloud-based virtual machines, it's like those servers are right on your local network, and your users can get back to work—from almost anywhere in the world.

Again, this *requires advance planning*. You need to know how you'll notify the vendor, what servers will be recovered, and you'll need to know how to connect to those servers once they're running in virtual machines. Documenting this information in advance will make it easier to implement when the need arises.

This is *more than just backups*—your cloud vendor has to not only offer storage but also the virtualization, networking, and expert services to recreate a portion of your production environment, virtually, in their own data centers. *Many vendors selling cloud-based storage are not selling complete disaster recovery*, even though they'll use the term “disaster recovery.” Just be aware of what you're buying. Vendors such as i365, EMC, iland, and others offer true disaster recovery in addition to cloud-based backups; even services like Amazon's E3C cloud-computing platform can be used for certain limited disaster recovery scenarios.

The Vendor Connection

There are several vendors who can make cloud storage and data protection a reality today. Some of them include:

- i365
- Iron Mountain
- Barracuda Networks
- CommVault
- EMC
- iland
- Unitrends

Different vendors approach cloud storage in different ways. Many provide a hardware appliance or software that you install in your data center, which replicates data to the vendor's cloud-based storage network. Some vendors specifically target small- to midsize businesses and provide solution tailored for them. i365's EVault is one example of a solution tailored for that business market. Other vendors target larger enterprises and provide more complex solutions designed with very large businesses in mind.

Do keep in mind, though, that as with any product or service you're evaluating, not every vendor is created equal. Ask yourself:

- How long has the vendor been in business? Who are their existing clients? Are they a stable company? Will they be around in 5 years, or 10?
- How long has the vendor offered this kind of solution, and how long have they worked in data protection? With the hype around “the cloud,” a lot of brand-new companies are playing in the cloud storage space and may not have the experience or track record you need to see in order to trust them with your data.

- Does the vendor offer a range of solutions or just a one-size-fits-all offering? Different solutions—software as a service, managed services, appliances, software, and so forth—offer flexibility to more precisely match your business’ particular needs.
- Is the vendor’s network solid? Look for geographically-dispersed, redundant data centers. You can also look for SAS70 Type II certification, which certifies an organization’s ability to audit and maintain their internal management controls—a critical capability when you plan to trust them with part of your business.

Be careful of offerings that seem “too good to be true,” especially from newcomers to the space. Cloud-based storage is a competitive, growing industry, but you should still expect to pay a fair price for a quality product from an established vendor.

Here’s Your New Storage Plan

In the next and final article in this series, we’ll look at different models you can consider for cloud-based storage and data protection. I’ll outline specific business advantages of each, and help you start thinking about a solution that will fit your needs.

Article 3: Leveraging the Cloud for Storage and Disaster Recovery: Three Practical Strategies

How will you incorporate cloud storage into your storage and data protection plans? Let's look at three common models—and some variations—that fit the bill for various types of business needs.

Keep Everything in the Cloud

One approach is to simply stop storing data locally and to keep it all in the cloud. You'll work with it directly in the cloud—often through a VPN connection or by means of client software installed on your client computers—and the data is simply protected all the time by the vendor's storage network. It's rare to see businesses rely solely on cloud storage for *all* their storage needs, but for certain categories of data, it can make a lot of sense.

There are some potential downsides. Depending on your Internet connection, accessing data in this fashion may be slower. If the data can only be accessed through a server application—such as a database server—then storing the data only in the cloud may not be practical. Cloud storage space costs, so storing a great deal of data may be more expensive than you can afford. However, be sure to also consider the costs of protecting that data when it's living locally, because you won't have to pay that overhead when the data is solely in the cloud.

This is, frankly, a pretty rare approach—at least in terms of storing *all* of a company's data. That would be expensive and probably impractical. That's why it's more common to see hybrid approaches that use the cloud more judiciously and strategically—something we'll get to in a moment.

Use the Cloud as a Backup

Another approach is to simply use the cloud as a giant backup device. Typically, this involves installing an appliance or software in your data center. That device is responsible for capturing the data, compressing and de-duplicating it, and transmitting it to the cloud. Appliances such as the i365 EVault Plug-n-Protect and Barracuda Networks' Barracuda Backup Service, are examples of this kind of appliance.

You continue to use your data locally. You're only relying on the cloud as a backup—a convenient, more automated way to get backups off-site than those antiquated magnetic tapes. If you need to recover data—either a single file or an entire server—you retrieve the needed data from the cloud. In the event that you need to recover a *lot* of data, your vendor may offer you the option of having it shipped to you. If that's an appealing idea (and it can make recovery faster if you have a slower Internet connection), be sure you choose a vendor that offers that option.

This is a very common model; the majority of the cloud storage vendors out there are primarily selling this model and calling it “disaster recovery” (technically, it isn't, for reasons I pointed out in the previous article). And this is a good model if it fits your needs. However, it puts all your data into one class, and assumes that you can tolerate some level of downtime for all your data. That isn't always the case for every business, which is where hybrid approaches come in.

Hybrid Approaches

Not all data, as I wrote in the previous article in this series, is created equal. That's why hybrid storage approaches are more common: They recognize that some kinds of data will need to be treated differently than others. Once you classify your data, you can choose a hybrid approach for each category, balancing cost, protection, potential downtime, and ease of access.

Onsite-Prime

In this model, you rely primarily on on-site data, and use the cloud only for backups. However, for certain critical categories of data, you might use the cloud as primary storage. Doing so makes that data more readily accessible from multiple locations, and ensures that you won't ever experience any downtime with regard to that data.

Cloud-Prime

In this variation, you keep most of your data primarily in the cloud, and access it directly from there. However, you also keep a local copy on-site. In the event that the cloud is unavailable—because you've lost your Internet connection, for example—you can use the local copy of the data as a backup.

For this model to work, your cloud storage provider needs to be able to replicate data *down* to you, rather than *up* from you to the cloud. In other words, as you work with data in the cloud, that data needs to silently stream down to some local storage device in the background so that it's up to date should you need to use it.

Other Hybrid Approaches

There's really no “line” when it comes to building your own hybrid approach. Keep some data live in the cloud, use the cloud to back up other data, and keep local backups of some cloud-based data. You can paint the picture however you want to in order to meet your specific business needs.

This is, in fact, the *value of planning ahead*. You can take the time to consider the different types of data you have, consider how important it is to you, and consider how much you want to invest in protecting each different category of data. You can then assemble the precise cloud storage and data protection plan that most exactly fits your needs.

Hybrid Details

I do want to caution you as you consider a hybrid approach because you want to carefully avoid creating a model that, combined with a particular vendor offering, creates *more management overhead* for you. A hybrid approach means multiple ways of dealing with data; for some vendors, that means offering you multiple solutions that may or may not integrate tightly or be managed as a single unit. If you're considering a hybrid approach, try to find a vendor that can offer you a *single* solution that implements the approach you want. You'll find that management becomes less intensive and easier, helping to ensure that your hybrid approach is successful.

Do be aware that some vendors *componentized* their product offerings; that's not quite the same thing as separate solutions. In other words, when you buy a car, you may want options like leather seats and cruise control, but you want them all installed and integrated into the final product. You don't want the car to arrive with no seats, and then receive a crate containing the seats later for you to "integrate" yourself. Talk with vendors to understand whether they're offering you completely separate, standalone point solutions, or whether they can offer you a fully-integrated product and service solution that has the options you need.

Conclusion

Cloud storage offers exciting new options for data protection and disaster recovery. With careful advanced planning, you can ditch those old backup tapes while providing better protection and faster recovery for your data—including broader accessibility, and even options for off-site disaster recovery, such as the "warm site" recovery model I described. All you need to do is:

- Take some time to think about and understand the data in your organization
- Work with vendors to understand the options they offer
- Create a customized model that meets your budget, data protection, and disaster recovery needs

We no longer have to put up with the constraints that tape backups have imposed on us for years; we can have the data protection capabilities our businesses have always needed—thanks to the cloud.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.