Redmond Channel Partner
DRIVING SUCCESS IN THE MICROSOFT PARTNER COMMUNITY
A SPECIAL REPORT FROM THE EDITORS OF RCP

MSP'S GUIDE TO

Rethinking Backup for the Cloud

Here are two dozen tips to help managed services providers make the most of the mind-bending proliferation of backup, recovery, availability, storage, archiving, file sharing and disaster recovery options that are enabled in the cloud. **By Scott Bekker**

ONEPHOTO/SHUTTERSTOCK.COM

THE RATE OF INNOVATION around backup has been nothing short of astonishing in the last decade. The explosion of highly available and relatively affordable public cloud offerings has led to a parallel proliferation of options for storing data in the cloud. Lines are constantly blurring in the cloud between backup, recovery, availability, storage, archiving, file sharing and disaster recovery (DR).

Savvy managed services providers (MSPs) are constantly finding new ways to turn those possibilities into profitable parts of their business. If you haven't rebuilt your managed services to take advantage of cloud backup, it's a great time to start. Even if you have a cloud backup, the baseline capabilities are moving so fast that it's pretty much always the right time to take another look at the way you're doing things.

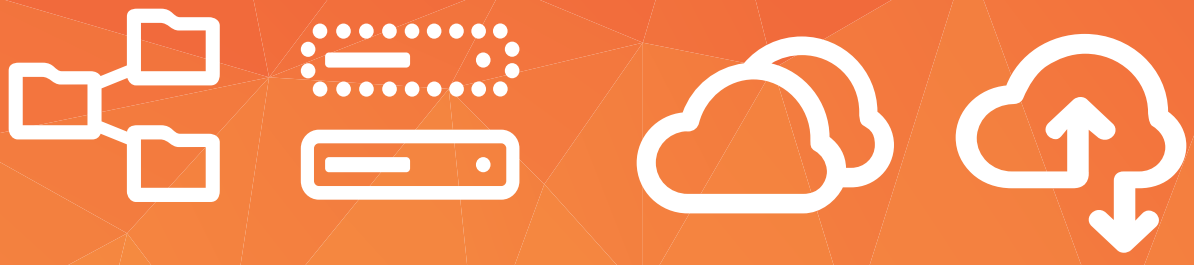
Here are 24 tips for rethinking backup in this cloud era.

1. OFFER BACKUP

The most basic tip is to make sure your MSP business is on this gravy train. There was a time not long ago when a good backup-and-recovery business line required an MSP to build and maintain its own expensive datacenter for off-site backup. No more. With a cloud provider for off-site backup copies, the capital investment required to get into the backup business is pretty close to nil.

AXCIENT™

efolder



The Channel's Most Powerful Suite of Data Protection Solutions

BUSINESS CONTINUITY

FILE SYNC & SHARE

CLOUD-TO-CLOUD BACKUP

FILE BACKUP & RECOVERY

To find out more, visit us at www.efolder.net

2. MAKE A BUNDLE

Speaking of the business side, one of the best ways MSPs make profits is by avoiding a la carte arrangements, and bruising item-by-item price discussions with customers. Instead, they package a lot of services together with one price tag. Cloud backup services are a logical service to bulk up just such a bundle. For MSPs who are also Microsoft Cloud Solution Providers, online backup is a great way to start creating that one-price package that moves the MSP's service away from the standard Microsoft price list.

3. TRY A WHITE LABEL

One more business note, as an MSP, you're a hot commodity. A lot of backup vendors try to sweeten the pot by allowing you to label their backup portals and interfaces with your own branding. Like bundling, it's another way to keep customers thinking about you as their key partner, rather than all the vendors whose tools keep things running behind the scenes.

4. FAST TRACK TO 3:2:1

The 3:2:1 rule is a staple of backup literature, but it could be an expensive and difficult rule to implement in practical terms. Three copies of the data in two different types of media with at least one off-site. For MSPs backing up customer data locally and to a public cloud, the difficult multi-media and off-site requirements are already handled. Consider that many of the major public cloud providers back up their data, as well, and you're looking at a lot of built-in redundancy.

5. SLA OF CLOUDS

Maintaining a datacenter is a tricky business. For many MSPs maintaining their own datacenters was a challenge due to the need to hire datacenter talent, keep hardware up-to-date and match the ever larger storage demands. Public cloud providers have all that down to a science, meaning they can offer insane levels of uptime.

6. REMEMBER TO BACK UP OFFICE 365

There's a widespread belief that for major Software-as-a-Service (SaaS) applications like Microsoft Office 365, you don't have to back it up. True, SaaS providers, like Microsoft in the case of Office 365, do perform some base-level backup of the service, and the service uptime is extremely reliable. Yet there are important gaps in the vanilla backup coverage that MSPs should look to fill.

7. ABILITY TO MAINTAIN ONLY ONLINE BACKUP

A lot of the newer solutions present opportunities for MSPs to offer only online backup. For born-in-the-cloud clients and in other cases, a cloud-only solution—where the organization's data is exclusively backed up in the cloud—is an option.

8. WATCH YOUR SPEED

Those cloud-only solutions have one glaring weakness, and that's the speed of recovery. In a real disaster where a bare metal restore is required, physics exerts itself. The speed of light and the bandwidth of the physical cables connecting the customer site to the nearest cloud provider's datacenters are a limitation. Having local backup options (that aren't also destroyed by whatever caused the crisis) can mean recovery in hours versus days, depending on the amount of data involved.

9. SUBTRACT SHIPPING TIME

The other side of the coin is that cloud-reliant backup and recovery solutions take the shipping time that it takes for physical tapes from a remote site to the customer site out of the DR timeline.

10. SPIN UP VIRTUAL DATACENTERS

A real game changer in the online-only versus local or shipped backup tapes debate is the high-availability technology that's part of many virtually focused backup and recovery solutions. Those solutions that allow your customer to spin up their entire environment in a vendor's cloud take the whole speed-of-backup discussion off the table. If a customer can run its business full-tilt in the cloud while the MSP diligently restores the local environment, it doesn't matter quite as much if that physical process takes hours or a day or two.

11. DEFEND AGAINST RANSOMWARE

The constant waves of ransomware attacks over the last several years cry out for a three-prong defense—backup, end-user training (short version: "If it could be a trick, don't click") and patching. Regular cloud backup can cover the backup element of that ransomware defense strategy.

12. BUT DON'T GET COMPLACENT ABOUT RANSOMWARE

Do be aware that a few strains of ransomware, like the Samas family, have been known to worm their way into backups. Some vendors are concerned that more ransomware will be coming with time-bomb capabilities that trigger after a long delay, making them potentially very difficult to extricate from backup files.

13. MIND THE AIR GAP

That ransomware issue raises one red flag about backup and recovery with cloud. At least with off-site tape there was an air gap aspect to backup, where there was no possibility for anyone to interfere with the backup files in an off-site storage facility. With cloud, there's always a connection. That's something to keep in mind for the paranoid.

14. MERGE THAT ARCHIVING

Archiving has historically been a different process than backup. The ability to keep searchable files around for a specified period

of time for legal or regulatory reasons is generally a separate class of software-engineering problem than backup. Some vendors are able to blur the lines with creative cloud solutions, or at least bundle products to help MSPs handle both needs.

15. SHARE FILES

Another area of blurring is with file sharing, where backup vendors have file-sharing solutions and elements of the solutions can overlap, or at least an MSP can bundle the services into a combined offering with enterprise file-sharing features.

16. OFFER SELF-SERVICE FILE RECOVERY

A nice-to-have feature of many backup solutions is the ability to allow users to perform self-service recovery of individual files in the case of accidental deletion or file corruption. With cloud offerings, this isn't always a given, depending on how the backups are created, but some architectures will allow it.

17. START ORCHESTRATING

One emerging area is the ability to orchestrate backup and availability activities through the cloud. A particularly interesting use case would be the ability to do something like track a weather feed and use things like local hurricane warnings to automatically spin up a hot standby site remotely until the storm passes. That's a bit futuristic, but automation features are becoming baked into many cloud technologies.

18. TAKE ANOTHER LOOK AT DR

Back to the MSP datacenter expense issue, MSPs who avoided DR due to the expense of maintaining their own datacenters as secondary locations for customers now have a lot more options to offer DR. A main one is to use cloud backup as the remote location for a customer's DR plans.

19. SIMPLIFY WITH DRaaS

Those MSPs who don't want to reinvent the wheel on creating DR solutions of their own based on cloud backup have another option. Disaster Recovery-as-a-Service (DRaaS) solutions hand the whole issue over to a DRaaS vendor who takes care of the cloud backup and presents an interface and tools tailored to DR requirements.

20. WORK DIRECTLY WITH THE BIGS

When it comes to MSPs and cloud backup, a lot of solutions involve cloud backup-specific vendors. Behind a lot of those solutions are the giant public cloud offerings of Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Cloud and others. MSPs can work directly with those vendors to tailor their own offerings or for customers who prefer those big names. Ironically, expense can be an issue when dealing directly with the public cloud giants. The cloud backup vendors know the platforms in and out and may have volume-pricing arrangements with the public cloud vendors. MSPs working on their own may be more likely to fall into pricing traps triggered by unexpected volumes and other issues.

21. SUPPORT MULTICLOUD

Working with one public cloud vendor can be good. Working with two or more might be better. MSPs with enterprise customers may need to support multiple clouds, say, a combination of Azure and AWS or GCP and IBM Cloud. Pricing pitfalls are more likely to be an issue here, as it's even harder to stay on top of multiple vendor byzantine pricing. Yet developing that expertise in multiple clouds can only increase an MSP's value.

22. HELP WITH CLOUD MOVES

Portability issues between public clouds will become more important over time. MSPs with the ability to help customers move backups from one cloud platform to another to take advantage of price differentials or service innovations will be in demand.

23. UPDATE THE PLAN

A highly valuable service in the cloud backup era is updating the backup and recovery, business continuity or DR plan. Customers are moving faster than ever, constantly adding new cloud services, ramping up their data volumes and becoming more reliant on that data. Even a plan that is six months old is probably missing some major new data initiative, even at midmarket and smaller companies. MSPs who can come in and baseline the data environment to help prioritize backups can serve as a lifeline. Keeping that plan up-to-date on an ongoing basis is another valuable service for the MSP's bundle.

24. STEP UP THE TESTING

No discussion of backup is complete without a call for testing. The same forces that make it a necessity to update the backup plan make it an absolute requirement to test the backup process. Every new SaaS application in the mix, every new source of critical data is a potential breakpoint in a recovery scenario. As the backup plan evolves, the recovery-testing schedule must keep pace. MSPs that can build testing into their service offerings save themselves and their customers major headaches in the future.

Cloud backup is a bewildering and fast-moving technology area. That's a good thing for MSPs who can stop and rethink the value that the cloud provides for backup and related services and then help dozens or hundreds or thousands of customers to realize that value. •

Scott Bekker is editor in chief of RCP *magazine.*