Data Protection and Disaster Recovery for the SMB
An SSG-NOW Outlook Report

2014

By Deni Connor and Earl Follis
Client Relations: Phylis Bockelman, Joel Frankel

SSG-NOW
8815 Mountain Path Circle
Austin, Texas 78759
(512) 345-3850

SSG-NOW.COM

Note: The information and recommendations made by SSG-NOW. Recommendations are based upon public information and sources and may also include personal opinions both of SSG-NOW and others, all of which we believe are accurate and reliable. As market conditions change however and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. SSG-NOW assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors which may appear in this document.

SSG-NOW
TARGETED ANALYSIS

Outlook Report

Sponsor

Management Summary

Cloud computing capabilities are challenging basic IT truths that have held constant almost since the advent of the 8” floppy disk in 1971. As virtual versions of applications, networks, phone systems and storage capabilities migrate to and become commonplace in the cloud, opportunities abound for small- and medium-sized businesses (SMBs) to save money and take advantage of cloud-based services. One of the most significant business opportunities for SMBs is the ability to utilize the cloud for disaster recovery and data protection.

Disaster recovery has traditionally been an afterthought—or a cost-prohibitive wish-list item—for SMBs since the dawn of personal computers. Disaster recovery has always been an expensive, complicated process that requires companies to rent access to a facsimile of their IT infrastructure in a distant, protected facility with backup power, networking and phone systems. The complexity of disaster recovery planning in the unlikely case that something bad happens, whether it be a natural or man-made disaster, widespread virus infections, or even an errant squirrel frying your local electrical transformer, has prevented most SMBs from taking advantage of this critical protection of the computing core of their businesses. Cloud-based disaster recovery is in the process of permanently changing the SMB dynamic from “Gee, wouldn’t it be nice” to “Our company cannot afford the business risk of *not* having a cloud-based disaster recovery strategy in place”. For SMBs, cloud-based disaster recovery has become a no-brainer.

Just as disaster recovery has always been a financially-elusive option for SMBs, data protection has also been a major challenge for SMBs. Fortunately, the proliferation of online backup and restore services makes tape-based data protection a thing of the past for most SMBs. Of course, many SMBs didn’t or still don’t have the technical expertise to perform regular backups and restores of critical business data using a tape-based data protection strategy. Cloud-based data protection now provides companies of all sizes with a viable, cost-effective, easy-to-use option for backing up—and most importantly *restoring*—critical SMB data. Just as with disaster recovery, cloud-based data protection is not just a nice-to-have, the simplicity and cost-effectiveness of cloud-based data protection is now a no-brainer for SMBs.

The disaster recovery plan for many SMBs—if they even had one—was for many years as simple as the owner taking home the server backup tape in his briefcase, then exchanging it for an older backup tape kept somewhere at home. This manual method of rotating tapes was certainly better than nothing, but it left much to be desired if a disaster ever struck. Was the backup good? Could the file or files be recovered and restored? Does anyone even know how to restore files from the tape backup? What if the server itself was damaged or destroyed in the disaster? Did the company have access to server hardware to which backups could be restored? As, many SMBs quickly discovered when they were hit by data loss in the era of tape backups, the answer to some or all of these questions could easily be “No.” Failure to restore and recover from data loss typically meant failure of the business itself.

Cloud-based disaster recovery and backup/restore offer intrinsic insurance from these historical vagaries of SMB data protection. You get daily confirmations that your backups are successful. If you have a data loss, you can restore to any PC with an Internet connection, not just a server. Most cloud-based disaster recovery services offer testing of the recovery process in a virtual sandbox using network, storage and application infrastructure that simulates as a company’s production environment. Cloud-based data protection is such an easy process that SMBs can empower individual users with the ability to restore their own files at the user’s discretion. There is no longer any need to call a support number or fill out a form in triplicate just to restore a deleted file. In both cases, there is usually not a requirement for specialized, expensive IT expertise to initiate the recovery or restore process. In a business environment that typically struggles to find, retain and pay for IT expertise, online data protection and disaster recovery is the perfect solution for SMBs who recognize the importance of having a plan in place to protect the company.

If you own a pizza restaurant or run a doctor’s office or work in any of the thousands of small businesses in this country, you likely do not have dedicated IT staff. Some small businesses grow to become medium-sized businesses that might require more full-time IT expertise but that is certainly not a given in an uncertain economy. Owner-operators and other small business managers likely have just enough computer skills to keep the company operating day-to-day, but most SMBs have no idea where to turn when they suffer a disaster or significant data loss. With these factors in mind, this report highlights the available answers to this common SMB question: how does our IT staff protect the company’s computing assets if we can’t even afford an IT staff?

Driving Issues, Trends, History

The increasing popularity and technical capabilities offered by cloud-based computing is both driving and facilitating the proliferation of cloud-based disaster recovery and data protection. Once your computer infrastructure is virtualized and running in the cloud, it's just a logical step to cloud-based data protection and disaster recovery as a service (RaaS). Cloud-based data protection and disaster recovery make the job of supporting and utilizing your SMB computer resources easier and much more economical. We are entering a golden age of cloud-based computing that's sure to make life easier and cheaper for SMBs who recognize the business-critical opportunity to provide scalable, virtual infrastructure that enables data protection and disaster recovery protection via the cloud.

The history of disaster recovery/data protection for SMB

The history of data protection in the SMB space started with the release of the personal computer (PC) in the early 1980s. Back then, backup and restore commands were built-in to MS-DOS and relied solely on diskettes, first 5.25-inch diskettes, then 3.5-inch diskettes. As networking capabilities developed and the concept of a central computer, or server, became popular in the late 1980s, tape-based backup and restore was considered state-of-the-art technology because it replaced cumbersome diskette-based backups with much higher-capacity tape media. But, the advent of tape-based backups did not relieve the requirement for SMBs to actively manage their backup media of choice.

For the purposes of disaster recovery, your backup media needs to be verified, rotated and stored offsite on a daily basis. Thus, the burden of data protection and disaster recovery for SMBs rested squarely on the shoulders of entrepreneurs and business owners who typically had neither the time nor the expertise to properly manage their backups. The other failing of tape-based backups at that time was the failure of SMBs to adequately test their backups by attempting to restore backed-up files on a regular basis. Many small companies learned a very difficult lesson the hard way by assuming that as long as tape- or diskette-based backup completed without errors, the backed-up files would successfully restore in case of a disaster, or more commonly, the simple need to restore a file that had been accidentally deleted. Turns out that early tape and diskettes were not a very durable backup medium and attempts to restore files from backups routinely failed during the first two decades of personal computer use by SMBs.

The costs of downtime for SMBs

Downtime costs have gradually increased over the years, as the complexity and amount of data stored on SMB computers and networks grew. It is one thing to have downtime or lose data because the computer used to keep the company's accounting suffers from a hardware failure; it's quite another if you build your business around, for example, a PC-based point-of-sale system (POS). When your accounting computer fails, it's inconvenient but your company can likely continue to serve customers and make money while you recover your data and repair the affected computer. However, if your POS system crashes, your small business might as well close its doors until the problem is resolved. The loss of an SMB's computers means no revenue until all computers are restored and back in operation. Hence, the cost of downtime for an SMB is directly tied to the extent of which your company relies on computers for day-to-day operations.

In the 1980s and 1990s, many SMBs were just beginning to dabble in using PCs as part of their daily business operations. Today, most SMBs are totally dependent on PCs, networks, tablets and storage devices to run their business. Disaster recovery planners use a metric called recovery time objective, or RTO, to indicate the goal by which a company needs to be back up and running following a catastrophic data-loss or other data-related event. According to U.S. Census Bureau statistics, annual revenue for American SMBs averages approximately $377,000 per company. That means that the average SMB takes in a little more than $1,000 per day. If your SMB has an RTO of three days, your company will likely suffer more than $3,000 in lost revenues while recovering from a disaster or other data-loss event. That can be a huge financial hit for a small business that struggles for economic survival in the best of times.

Data protection and disaster recovery is still an afterthought for many SMBs

Of all of the activities that an SMB must perform in order to survive and thrive as a viable business entity, data protraction and disaster recovery are still likely to be an afterthought for many SMBs. This lack of emphasis on data protection and disaster recovery for SMBs is likely temporary; sooner or later a data loss or disaster will have a significant impact on business operations. Hence, a company that has already suffered a data loss or similar disaster is much more aware of the business-critical role played by data protection and disaster recovery in the ongoing operation of their business. For example, after the terrorist attacks on New York City on 9/11, many small businesses in lower Manhattan failed because of a lack of a viable disaster recovery plan that would have restored their business operations. Any company caught in that predicament no doubt learned a hard lesson in SMB disaster recovery.

Data protection alone is not enough to protect most SMBs

Data protection is certainly a good first step for any SMB but the real protection comes from a DR plan that not only restores data, but also restores any computing components affected by a disaster. In other words, data protection gets your files back while disaster recovery gets your business back. Prior to the introduction of cloud-based disaster recovery services, disaster recovery planning involved contracting with a disaster recovery company to temporarily provide hardware and software to replace hardware lost in a disaster. This concept was and is very expensive. However, now that virtual servers are commonplace in SMB computer infrastructure, disaster recovery can occur automagically in the cloud following a disaster or data loss event. Modern cloud-based disaster recovery services can take regular snapshots of your virtual infrastructure and restore those virtual components in as little as five minutes. This capability changes everything for SMBs looking for true disaster recovery, as opposed to data protection schemes that simply restore files to a directory.

The cloud makes RaaS a reality

Disaster recovery as a service (RaaS) is totally tied to and dependent on cloud computing to make it both economical and robust enough for SMBs to rely on in the case of a data emergency. Most managed service providers (MSPs) have been offering virtual server hosting to their SMB customers for more than five years, so offering a RAAS solution is a logical progression from having your server hosted in the cloud. RaaS offerings now support disaster recovery DR for virtual servers, applications, networks and storage. Your entire infrastructure can be backed-up as often as every five minutes and restored to an identical configuration in about the same amount of time.

RaaS also makes disaster recovery tests as easy as clicking a button. Disaster recovery tests are also much easier in a RaaS environment. While hardware-based disaster recovery tests take months to plan and can last for as long as two weeks, depending on your RTO, RaaS recovery testing can be performed in a matter of minutes. During a RaaS test, a complete copy of your virtual environment is created in a virtual isolated sandbox in the cloud so you can verify that everything will be configured correctly, should your disaster recovery plan ever be put into effect. This capability alone makes RaaS a very compelling offering for SMBs who might have never even had a data protection strategy in place, much less a disaster recovery plan.

Challenges for SMB disaster recovery implementations

The basic challenge for disaster recovery and data protection for SMBs has always been the relatively low level of technical expertise fond in the average SMB. Just making the leap from running their business on physical servers versus migrating to virtual servers in the cloud can be a significant obstacle for many SMBs. Smart RaaS vendors offer SMBs assistance in migrating their servers to a cloud-based architecture. There are also a number of computer resellers and consultants who can be hired to assist SMBs transitioning from physical servers to virtual servers to a comprehensive RaaS strategy. Once again, many SMBs who haven't been through a data loss event might balk at the cost of migrating to a cloud-based architecture but considering that the survival of the company depends on having a disaster recovery strategy in place, most SMBs simply cannot afford to not do whatever it takes to protect their computer infrastructure via RaaS. Federal regulations such as HIPAA require data custodians to have a disaster recovery plan in place.

SMB DR platform and network requirements

The migration from physical servers to virtual servers brings up important considerations that you need to keep in mind when moving your computer infrastructure to the cloud. What kinds of servers do I need in the cloud? What kind of networking do I need in the cloud? And, what kind of Internet connection does my location need to access my servers in the cloud? If you have critical software on which your company relies, you must make sure that your cloud provider supports those server operating systems. You must have enough bandwidth between your servers in the cloud so that performance is satisfactory. And, most importantly, you must have a reliable, and hopefully redundant, connection between your business location(s) and your Internet cloud provider. All three of these considerations must be taken into account while planning a migration to the cloud and your cloud provider, reseller or consultant can assist you with making those decisions.

RaaS offers scalable performance and capacity

In addition to the myriad benefits of moving your computer infrastructure into the cloud, none is more useful to a growing business than the capability to scale your server and network performance in the cloud to meet temporary or permanent business requirements. For example, you could work with your cloud provider to increase bandwidth or server capacity at specific times of the month or year to meet business requirements. A flower shop might want to increase their server and network capacity around Valentine's Day. An online vendor might want to increase performance or capacity during the holiday season, when demand is significantly higher. Being able to quickly and economically scale your cloud-based resources as needed without incurring additional capital expenses or without going through the process of acquiring and provisioning hard computer is a very attractive by-product of moving to the cloud. Your RaaS capabilities can scale just as easily as the virtual infrastructure itself, thereby saving time and money for cash-strapped SMBs.

Data Protection Essentials – On-premises backup

Data protection delivers exactly what you'd expect: protection, i.e. backup and restore, of company data in case of a data loss event. Data loss could be caused by a user accidentally deleting a file, malicious destruction of data from internal or external personnel, data loss due to a virus or other malware, or data-loss caused by a natural disaster. One of the good things about data protection is that the reason for the data loss is mostly immaterial compared to the need to quickly and easily restore the missing data from a backup medium. There are multiple on-premises backup strategies and technologies available today that address the problem of quickly and easily restoring lost data. There are also on-premises backup options still available that are not necessarily quick to restore or easy to administer, but they may still have a place in data protection-specific situations.

Backup to tape and disk

In the beginning of the computing revolution, backup and restore hardware for high-capacity computers was usually a tape-based technology. But, as the storage capacity of hard drives grew and the cost of hard drives decreased, the economic argument for cheaper, tape-based backups has been almost eliminated. With most desktop and laptop computers now shipping with 1 terabyte (TB) disk drives, even a high-capacity 5TB tape drive will be dwarfed by the data backup requirements of just a dozen average users.

Another historically common problem with tape-based backups is that you still have to rotate the backup media daily to an offsite location in case of a disaster. If your offices catch fire, you don't want your backup tapes to also go up in flames so you either hand-carry your backup tapes to another location daily, or you must hire a data storage company to handle retrieval, storage and return of your tapes on a set schedule. The increased cost and complexity of tape-based backups is no longer worth the trouble, particularly now that cheaper disk- and cloud-based storage options are now available. Storing your tape backups in a different physical location for safety also causes unnecessary delays anytime you need to restore files from a backup set.

That same economic argument against tape backups is also a strong argument for using disk-based technology for on-premises backups and restores. With the price of a 1TB hard drive now well under $100, on-premises disk-based backups are cost-competitive to tape-based backups and can be configured to run backups on an ongoing basis, rather than only doing a single monolithic backup overnight. Disk-based backup software and appliances can perform continuous backups anytime a change to a file is detected. The only downside to an on-premises disk-based backup strategy is the possibility of a disaster wiping out your data center, taking your backups with it. Many companies that have access to multiple data centers will replicate disk-based backups between geographically diverse data centers to avoid this risk.

Snapshot backups

Snapshots are a data protection technique that stores all of the details about a dataset, for quick retrieval. Usually, snapshots use data deduplication so that the complete dataset is only copied as part of the first snapshot of that dataset. Subsequent snapshots of that dataset only record the changes to the dataset, making all subsequent snapshot extremely quick to complete. Backup technology that supports snapshots can be on-premises disk-based or cloud-based, or a combination of the two approaches. Snapshots are particularly valuable for virtual servers, where snapshots have been utilized for years to store virtual machine (VM) configurations for cloning or backup purposes. Backup vendors have extended snapshot technology to now work seamlessly with physical servers, SAN arrays and other data repositories.

Instead of a once-a-day backup scheme, by utilizing snapshots, you can now backup your servers as often as you want with no discernible performance penalty. Restoring a snapshot can take a little longer because the full dataset must be reconstituted from all past snapshots then restored to the physical or virtual server as needed. This process is still much faster than any tape-based restoration technology and you have the granularity to restore a snapshot from a specific point in time. Snapshots are an important development in backup technology and should be on your list of requirements when searching for a suitable backup and restore solution.

Backing up virtual machines: images and clones

Image files are an all-inclusive copy of the files and data that make up a virtual machine (VM). You can leverage clone technology to distribute copies of images to multiple, identically-configured virtual servers. Images and clones are similar to a snapshot, except that images and clones are typically specific to virtual servers and they include the full dataset, rather than a full snapshot plus any data deltas recorded since that full snapshot was taken. Images first became popular in software test labs, as virtual servers became a reality in the early 2000s. If you needed to test your software on 12 Windows servers, you could build one virtual Windows server, create a clone of that VM image, then easily bring up as many identically configured VMs using that common clone.

Today, managed hosting providers such as GoDaddy and Rackspace use VM images and clones to dynamically provision identical virtual servers as customer needs expand. Do you want add Windows-based Web server to your hosted server farm? You can provision and boot that new server in a matter of minutes, as the behind-the-scenes process uses a cloned VM image to boot the new server. The same process works for Linux-based VMs. If you use virtual servers in your IT infrastructure, you should configure your backups to store all of your VM images for later restoration, if needed.

Continuous data protection

With new technologies and strategies in the market, continuous data protection is now a reality. Rather than your backups taking place once a day -- usually overnight -- you can perform backups of physical or virtual servers on a continuous basis. This continuous backup feature reduces the possibility that a deleted or corrupt file won't be part of a recent backup. Or, consider the situation of a traditional overnight backup strategy: If you create a new file or move an existing file to a different location during your workday, that file isn't going to be backed up until the nightly backups run, leaving your data exposed until a successful backup is completed. Continuous data protection performs backups at regular intervals throughout the day, or continuous data protection can even detect when a file changes or a new file is created and make an immediate backup copy of that file.

Redundant servers and failover

Another popular method of on-premises data protection is by using redundant physical servers or a server cluster to provide redundancy for business-critical server hardware and software, not just a backup data set from the contents of a server. Obviously, compared to data protection schemes using on-premises or cloud-based backup technology, redundant servers and server clusters are far more expensive. As a result, redundant servers have a steep 1-to-1 ratio of production server costs to backup server costs. Server clusters can reduce this hardware cost ratio somewhat, while simultaneously adding load-balancing capabilities to the equation.

If you have a cluster-aware application, you can run that application on a server cluster with multiple nodes and have the application load spread between the nodes. These are called active-active clusters. You can also run your server cluster as a an active-passive cluster, with one server being actively in use, while one or more backup servers wait for the command to become active in the event that the primary server node goes down. That process is called failover, when the active cluster node goes into a passive state while a passive, stand-by node takes over the active server role. Passive server nodes can them be taken offline for maintenance or repair activities. Server clusters give you the fastest recovery time of any data protection strategy available, but you are still exposed to considerable risk because the clustered nodes are typically located in the same data center. Data center interconnects now offer the possibility of locating cluster nodes in separate data centers but the cost and complexity increases dramatically in that type of architecture.

Application-specific backup

Whether or not you utilize on-premises backups, cloud-based backups or a combination of the two, the next option to consider is application-specific backups. Application-specific backups are valuable when you want to backup an entire application eco-system or even a software-as-a-service (SaaS) application, rather than individual files, VM images or physical servers.

For instance, Salesforce is a cloud-based business-critical SaaS application for hundreds of thousands of companies worldwide. Salesforce can be customized by users and integrated with thousands of third-party add-ons that extend the capabilities of the core Salesforce product. While Salesforce does provide redundancy of the core Salesforce application, Salesforce does not guarantee that your customizations and third-party integrations will be preserved and protected in the event of a hardware or software failure in the Salesforce infrastructure.

Google Apps is also now a business-critical application environment for many companies who rely on the collaboration capabilities and user desktop applications, such as document editing, spreadsheets and email. Vendors now offer full backup capabilities of entire SaaS application environments, such as Salesforce and Google Apps, with backup of other popular cloud-based applications coming soon. If your company relies on a SaaS application, ask yourself how you would approach a restoration of lost data for that application should a data loss occur in the cloud. Once your company comes to rely on SaaS applications, having a data protection and disaster recovery strategy in place for those applications becomes just as business-critical as traditional file and server backups.

Implementing RaaS for SMBs

Clearly one of the biggest opportunities for SMBs to implement a viable, cost-effective disaster recovery plan is via disaster recovery as a service (RaaS). RaaS allows you to not just protect your data, but to also have a tested method to restore your company's IT functionality in the event of a natural or man-made disaster that would otherwise halt company operations. RaaS allows you to create a virtual backup of your entire computing infrastructure, including physical and virtual servers, that can be restored in a matter of minutes should the need ever arise. RaaS also allows companies to schedule DR tests on an ad hoc basis, where all protected computers are restored into an isolated sandbox with the production IP addresses. Traditional cold-site DR centers are extremely expensive and it typically takes months to plan a DR test in the cold-site recovery center. That's all changing with RaaS and it to the benefit of SMBs, for whom a traditional cold-site DR strategy has never been an option due to cost. RaaS puts enterprise-level DR well within reach of SMBs.

RaaS pricing models encourage SMB adoption

The first consideration when formulating a DR strategy for your SMB is typically the cost of DR services. While RaaS may not be a good fit for large enterprise companies who have hundreds or thousands of computers that need to be protected with a DR strategy, RaaS is perfect for SMBs. RaaS vendors offer different pricing models that can be based on a flat fee for X number of protected devices, a monthly price per protected device or a monthly price based on the amount of data being backed-up. Or, your RaaS vendor may offer a combination of these pricing models, allowing you the luxury of picking the pricing model that provide the most service or the lowest price. The very nature of RaaS makes it ideal for a pay-as-you-go payment scheme. This means that you can tailor your DR pricing based on a count of protected computers each month, rather than having to commit to a yearly contract. Monthly pricing of RaaS means that you only pay for what you need each month and unused licenses are a thing of the past. Think of it as consumption pricing, where you only pay for what you use. RaaS pricing is already a relative bargain in the world of DR services and pay-as-you-go pricing makes it all the more attractive to SMBs.

Ease-of-use is key for SMBs

Of course, all of the RaaS functionality in the world is useless if it's so hard to use that SMBs can't get over the learning curve. This is where you need to carefully evaluate competing RaaS vendors and test their products hands-on to make sure that you will be able to perform the steps required to restore all—or part--of your computing environment when the time comes. So carefully evaluate ease-of-use characteristics when evaluating RaaS vendors and their DR management interfaces:

- Ease-of-use in configuring and managing your DR backup process on a day-to-day basis;
- Ease-of-use while testing the restore process (you will be doing this often); and,
- Ease-of-use in restoring your computing environment to a production-ready state

If you struggle with using your RaaS management console in any of the three situations above, that is a sign that you need to either get training on your RaaS vendor's management interface, or you may need to select a different vendor who has software that is easier-to-use. History tells us that software that isn't easy to use, especially in the SMB market, tends to not get used at all. Make sure that you are comfortable with your RaaS software or hire an IT company to help you manage your DR backup and recovery process.

VM snapshots and recovering VMs

The cornerstone of RaaS is the ability to take regular or ad hoc snapshots of your VMs and archive those snapshots for immediate retrieval when/if the time comes. With RaaS and the ability to take snapshots many times per day, one of the challenges of restoring your computing infrastructure is being able to identify exactly which snapshot of which VMs is the one you want to restore. The quickest way to answer that question is figure out exactly when you began to observe issues in your IT operation and pick the snapshot just prior to that point. This is where the ability to quickly test the RaaS restore process becomes very helpful. Because of the ability to quickly pick a restore point to test in an isolated sandbox, there is no downside to picking a restore point from your available snapshots, letting it run in the sandbox and then decide whether or not this recovery point object (RPO) goes far enough back in time to resolve whatever issues from which you are trying to recover.

Once your sandbox-recovered environment is operational, then you can evaluate whether or not this specific snapshot will suffice to get your computers operational again, or if you need to go back in time a little further in order to correct whatever issue befell your computers to begin with. The ability to easily and quickly take multiple snapshots every day means that you have a lot of granularity in choosing your RPO.

Though we are talking about VMs in great detail, many RaaS vendors offer what's called bare metal recovery as an option, as well. Bare metal recovery allows you to restore an image taken from a physical server and restore it to a point in time in the past. Bare metal recovery is initiated through a bootable CD or thumbdrive and restores the entire software configuration and data from a backed-up production server to a physical server in your office, an MSP's or a co-located data center. This process is not a quick as that for restoring VMs but it is still the quickest method for recovering physical servers to a chosen RPO. If your IT infrastructure uses physical servers, be sure to carefully consider the capabilities of your chosen RaaS vendor to perform bare metal restores in the event of a disaster.

Automated, recurring virtual DR tests

As mentioned, another invaluable feature of RaaS is the ability to schedule virtual DR tests on a regular or ad hoc basis. We recommend you run a virtual test of your RaaS restore process at least once a month if you've made no configuration changes, or as soon as possible after any significant configuration changes to your computing infrastructure. For example, if you add a new server, change data centers for physical servers, or change MSPs for a hosted or virtual server, running a DR test as soon as possible after said change is the best way to insure that the RaaS restore process continues to give you the protection you expect and pay for. Historically, the biggest single mistake companies make regarding data protection and disaster recovery is not fully testing the restore process on a regular basis. On-demand virtual DR tests make this previously difficult, expensive testing procedure so easy and quick that SMBs have no excuse for not regularly verifying that their DR recovery strategy is working as designed. With most RaaS software, executing an ad hoc DR test is as easy as clicking your mouse a few times in the RaaS management console, then verifying the results. Your RaaS can help you configure and complete regular DR recovery tests.

SMB DP/DR Use Cases

Data Protection (DP) and disaster recovery (DR) and DP for SMBs falls into several distinct use cases, or situations that fit the capabilities and features of DP/DR for SMBs. These use cases are not intended to be an all-inclusive list of viable applications for DP/DR for SMBs, but rather representative examples of how and why SMBs should consider DR and DP solutions to protect their company data. The real goal of a DP/DR strategy is to ensure business continuity in the wake of a disaster or other data-loss event. With that goal in mind, the basic requirement for a business continuity plan is to have a secure, available backup copy of all of your business-critical data. Beyond the restoration of lost data, the next rung on the DP/DR ladder involves restoration of business processes. Your DR business continuity requirements can be addressed by a RaaS solution, or perhaps via use of a DR cold- or warm-site strategy. These use cases should help the reader recognize where and how available DP/DR solutions can be leveraged to recover from loss of company data or interruptions to business operations.

SMB using only DP

Use of cloud-based data protection for most SMBs is now so cost-effective as to be considered a proverbial no-brainer for businesses that in the past might not have had viable DP options. Average prices to protect 50GB of data on a single computer are now well below $100 per computer, and some DP vendors offer additional discounts for multiple computers protected via the same shared company account. For less than $8 per month per protected computer, you can have a backup copy of critical business data on those computers. Considering that a single data loss event can cost your SMB hundreds or even thousands of dollars from which to recover, if recovery is even possible, every computer in your business should have a subscription to a DP service and you should backup all critical data at least twice per day.

One additional benefit to most DP services is that it not only gives you a cloud-based backup copy of your critical data, it also gives you remote access to all of your protected files. Because most DP vendors are using a cloud-based back-end to backup critical data, you can now access those backup files from any Web browser in the world. You no longer have to save copies of a presentation or important documents on a USB thumbdrive and hope that it doesn’t get lost or stolen while you travel. Using cloud-based DP, you will be able to access your cloud-based backup files from any place that has connectivity to the Internet, including from your smartphone. This capability is yet another reason that DP for SMBs should be considered the new-normal standard as a first-tier business continuity strategy.

Recovery-as-a-Service (RaaS)

RaaS appeals to many SMBs as the next logical step beyond data protection of their company's digital assets. RaaS is ideal for companies that use virtual servers as part of their computing infrastructure, though RaaS has applications for companies that only use physical servers, or companies that use a combination of virtual and physical servers. RaaS copies not just files to the cloud, RaaS can also create copies of virtual machine images and even bare-metal recovery images. Virtual machine images can be restored in a matter of minutes in the event of a disaster. For example, if your company uses VMware, Citrix XenServer or Microsoft Hyper-V virtual servers, a RaaS service can make and retain copies of your VM images called snapshots, each representing a specific point in time. You can configure your RaaS service to take VM snapshots on a regular basis, say several times per day, or on an ad hoc basis, say just before performing a major software upgrade or installing a new application.

With RaaS, rather than just having backups of files, you can capture both the data and the configuration of each server in your computing infrastructure. When you go to restore a VM snapshot, you are restoring the server and its data to the exact configuration and operating state when the snapshot was taken. The only real concern when restoring a VM snapshot is deciding which snapshot to use. This decision usually takes into account an analysis of when things began to go wrong, though with RaaS you can easily restore a snapshot, test it to see if resolves the issue, and if not, simply choose an earlier snapshot to restore instead. The same process is true with bare-metal restores: You can schedule regular as well as ad hoc snapshots of physical servers and restore those to a similarly-configured physical server in the event of a disaster. A bare-metal snapshot is a little more complicated to restore than is a VM snapshot but you should be able to successfully perform a bare-metal restore in a few hours.

The other obvious advantage to RaaS for SMBs is the ability to schedule and perform virtual DR tests on an ad hoc basis into an isolated sandbox, as a verification that the RaaS service is working as designed. Virtual DR tests of VM snapshots are very simple to initiate and should cost your company nothing, other than the time it takes to perform the test. Testing is the most important step of any DR plan: You have to regularly test the ability of you and your RaaS vendor to successfully restore your virtual server infrastructure. If your RaaS strategy includes bare-metal snapshots for physical server, you must also test your ability to restore a bare-metal image are least twice a year. Unlike cold-site DR tests that are time-consuming and expensive to conduct, your RaaS plan should take advantage of the fact that virtual DR tests can and should occur on a regular basis.

SMB using a DR cold site

There are still specific situations where the old-school DR strategy of having a subscription for access to a cold-site is still considered a best-practice. SMBs may need to subscribe to a cold-site DR plan if they have specific, expensive hardware in their infrastructure that cannot be effectively duplicated in a RaaS environment. If, for instance, your company has a high-performance storage area network (SAN) that stores business-critical data, having the ability to quickly restore that data to a SAN located at a hosted cold-site will be far more cost-effective than the company buying a complete standby SAN configuration that may or may not ever be called into use. That stand-by SAN will also have to be housed in a data center that is far enough away from the main company data center that a regional disaster won't wipe out the backup SAN along with the production SAN.

In those situations where a cold-site DR strategy is indicated, be prepared for both the annual cost—based on the hardware required and the RTO specified--and the amount of work required to develop a cold-site DR plan. Also, note that cold-site DR plans must be fully tested at least once a year, preferably twice a year, and the process of testing a cold-site DR plan can be complicated and challenging. Although the cost and complexity for cold-site DR is higher than for RaaS DR strategies, if you fall into the category of needing access to a DR cold-site in the case of a disaster, the cost and complexity is well worth it should a disaster occur.

Other DR Considerations for SMBs

There are additional considerations for SMBs jumping into the world of DR or DP. Understanding the importance of RTOs, replacement hardware, business continuity and regular testing for your DR or DP plan is crucial. Each of these considerations contributes to the overall robustness and effectiveness of your DR or DP plan. This primer will help you better understand the various terms and concepts required to implement an effective DR or DP strategy. Your DR or DP vendor is an excellent resource for further information on each of these topics.

Recovery time objectives for SMBs

The recovery time objective (RTO) is an important measure and goal of your DR planning process. RTO measures the time and level of recovery you expect to achieve after a disaster or data loss event. Of course, all companies want to recover from a disaster as quickly as possible but the physical realities of the recovery process dictate that your DR plan take into account a realistic amount of time to complete the disaster recovery process. Of course, restoring VMs from snapshots, performing bare-metal restores, and acquiring or provisioning new hardware all takes time. With cold-site DR planning, your RTO may be constrained by the ability of your DR vendor to make a cold site available and have all of the hardware configured as specified. It is important that you choose a realistic yet aggressive RTO during the DR planning process, as the RTO can affect how much our DR plan costs the company. In general, the shorter the RTO, the more money it will cost to achieve. DRaaS offers the quickest RTOs for VMs and bare-metal restores, but those RTOs are still bound by the amount of time it takes to deploy replacement computer hardware and complete bare-metal restores.

Planning for the loss of hardware in a disaster

If your computer infrastructure is based solely on VMs, you will likely have no DR requirement for replacement hardware save whatever networking gear connects your SMB to your DRaaS provider. If some, or all, of your computing infrastructure includes physical servers, then you must include in your DR planning a strategy to replace hardware damaged or destroyed in a disaster. Your hardware replacement strategy could be as simple as expedited ordering of replacement hardware from a major PC vendor ASAP after a disaster—but you'll have to include in your RTO the time required to order and receive the replacement hardware. Or, you might choose to use a cold-site DR vendor to provide temporary access to replacement hardware during a disaster, or you might choose to have working spares of all your computer hardware safely stored far enough away to be safe in a disaster, yet closely enough that the hardware can be retrieved and put into service in a timely manner. If you choose to procure and store replacement hardware, be sure to also include frequent testing of those spares in your DR plan. There is nothing as useless and expensive as spare hardware that will not boot-up when you need it.

Does your SMB need a DR cold site?

If your SMB computing infrastructure relies on physical servers, you must have a hardware replacement strategy in place as part of your DR planning. If you have already ruled out ordering new hardware as soon after a disaster as possible or purchasing spare hardware for use in the event of a disaster as viable strategy for replacing inoperative hardware, you should then start shopping for a cold-site vendor who can provide temporary access to similar hardware. Cold site DR vendors maintain a large inventory of computer hardware in protected data centers to which your SMB can gain access during a disaster, but you have to have a cold site service contract in place *before* disaster strikes your company or your physical location. Cold-sites can offer RTOs as short as 24 hours for making hardware available and allowing you to get it configured and operational following a disaster declaration.

Especially in the event of an area-wide disaster, e.g. a flood or other natural disaster, every company that subscribes to cold site DR services will be competing to for space in the recovery data center. Cold site vendors will typically turn away new DR customers during an actual disaster. Think of cold site DR services as an insurance contract. You can't buy insurance to cover a risk that has already occurred, otherwise, no one would ever buy insurance. Your DR "insurance" must be in place before the covered event happens.

DR testing

Testing of the DR plan is the bane of any DR planner, yet it is also the single most important aspect of your DR plan. A DR plan that is never tested might be hiding the fact that your DR plan is insufficient, incomplete or ineffective when the disaster hits the fan. Assuming that your SMB will eventually fail if you cannot resume business in a timely manner following a disaster, that is not a risk you can afford to take. If your DR plan relies on VM snapshots, running a DR test is typically as simple as clicking a button in the DR vendor's management console to restore your VMs to a sandbox and verify operation is as expected.

If your DR plan includes bare metal restores, then you must test your bare metal restores on a regular basis as well. We recommend that you perform bare-metal restore tests after every major change to the hardware or software configuration of a physical server. In the absence of major configuration changes, we recommend that you test the bare-metal restore process for each of our physical servers at least once a month. If you subscribe to cold site DR services, your contract with the DR vendor will include a schedule for DR test(s). Considering that cold site DR tests require cold site vendor employees to provide their expertise and time during your test, more frequent testing costs more money. As a result, most cold site DR vendors offer one DR test per year, with additional tests available on a pay-to-play basis.

DP recovery testing

If a true DR plan is beyond your budget, an SMB might choose to implement a data protection plan instead, under the assumption that having a copy of your critical company data in the cloud is far better than no data protection at all. A DP plan backups up all files and business-critical company data on a regular schedule that you can configure. Once the initial backup of a computer is uploaded to your DP provider, all future backups are differential in nature, i.e., you do not perform a full backup of 50GB of data on your desktop computer every time you run a backup, you are only backing up the data that

has changed since the last backup. DP vendors fine-tune this concept using de-duplication technology that prevents sending redundant data up to the DP cloud. As a result, you can configure your DP backups to run several times a day with little impact to your protected computers.

Just as DR testing is critical to verifying that your DR recovery plan will work as expected when it's needed, regular testing of your DP restoration process is also critical to verifying that your data is being protected as expected. At least once a month, you should browse your cloud-based DP repository and attempt to restore multiple files from multiple directories to a local computer directory. This testing will tell you whether or not your files are being protected and that those files can be restored when needed. When you perform a DP test, be sure that you do not overwrite the original files on your local hard drive. Remember that DP strategies also make backed-up files available from any Web browser or mobile device. If you do not avail yourself of this feature on a regular basis, you should also test your ability to access and download files remotely at least once a month.

Business continuity for the SMB

The last consideration for your DR planning is developing a strategy for business continuity in the event of a disaster. Business continuity planning requires you to think one step beyond DR recovery of your IT assets and data. Business continuity planning answers the question "How do I restore my business operations in the event of a disaster?" Your recovery plan should include how and where your employees answer company phone calls or access company email following a disaster. If, for instance, your company has five employees working daily in a company office, you need to have a plan to return those employees to productivity as soon as possible after a disaster. Perhaps your business continuity strategy can rely on employees working from home following a disaster, or perhaps you need to contract with a DR cold site vendor to provide cubicles, computers, Internet access and phones to affected employees. In some respects, business continuity if the most critical phase of your DR planning as an effective business continuity plan provides for your company to start providing your customers with their products or services as quickly as possible. Time, as they say, is money and the longer it takes your SMB to get back to the business of your business, the more costly it becomes in terms of direct financial losses and the loss of customer goodwill.

Best Practices for the Implementation of DP/DR for SMBs

Luckily, SMBs do not have to reinvent the wheel when implementing a viable, cost-effective DR or DP plan. Your company can leverage the experience, both good and bad, of thousands of companies who have crossed this same bridge before. This old adage about wisdom certainly describes the DR and DP planning process: Making good decisions comes from wisdom, while most wisdom comes from making bad decisions. Leveraging the wisdom of multitudes of companies that came before you, we offer some common—and uncommon—sense guidelines for how to plan and execute a DR or DP plan for your SMB.

- **Identify the problem:** Before you can choose the proper DR or DP strategy, you must first identify the business, computing infrastructure and data-loss risks to your business operations in the event of a data loss event or disaster.

- **Evaluate your options:** First decide whether data protection will suffice to protect your business or whether a disaster recovery plan is required. The price differential of DP versus DR is becoming narrower, so don't necessarily rule out DR until you've considered all options.

- **Find a good partner:** Once you know what type of solution you need, research online and find a good DP/DR partner that meets your needs. Contact at least three vendors and see how responsive they are to your requests for information and quotes. A company that doesn't provide timely, accurate responses to your inquiries before you buy will likely not respond in a timely fashion after you are a customer and are in the midst of a data loss event or a disaster.

- **Develop your DP/DR plan:** Your DP/DR plan should be printed on paper and copies should be stored offsite in a safe place, as well as retained in electronic form. The paper copies might be your only accessible version of the DP/DR plan should a physical disaster affect your primary place of business or the data center where your data resides.

- **Your DP/DR plan must include business continuity steps:** Remember that just restoring VMs or restoring missing files and data is probably not enough to restore your business operations, i.e., you still may not be able to generate revenue and service your customers. Include in your DP/DR plan recovery actions to restore your business phones, access company email, monitor website orders and inquiries, and provide a physical location for your employees to work should their primary offices be unusable. For instance, a doctor I know keeps paper copies of patient information and office visits forms handy in case their electronic medical records system is ever inaccessible during the hours they see patients.

- **Keep your DP/DR plan updated:** Most SMBs operate in a constant state of flux and change. As your computing infrastructure and business strategies change, be sure to update your DP/DR plan accordingly. When and if a disaster or data loss event occurs, you will not have the time or resources to track down new server info since the last plan update or data stored in a new location. We recommend scheduling month reviews of your DP/DR plan in accordance with your recovery plan tests.

Share your DP/DR plan with your employees: Disasters or data loss events can happen at any time, even when the owner or responsible for DP/DR is on vacation. You should have a back-up DP/DR administrator who is familiar with the recovery plan in case the primary responsible person is not available when the plan is put into effect. Beyond that, *every* employee should now that a DP/DR plan exists and what their specific responsibilities are in the case of an emergency.

- **Test, test, test:** No matter which protection strategy and vendor you select, you absolutely Must perform regular tests. If you choose a DP solution, be sure to test the restore procedure and access your cloud-based backups remotely at least once a month. If you choose a RaaS solution, execute a DR test at least once a month. If you select a solution that includes a cold-site recovery strategy, be sure to do a full test of your DR plan at least once a year, more often if you can afford it.

- **Communicate with other SMBs:** There is strength in numbers and the Internet offers SMBs the ability to learn from the DP/DR preparations of other companies in a similar situation. Your DP/DR vendor likely has a support forum or user group where companies can share their experience, concerns and strategies. Join, contribute and participate so that you can learn from what other companies are doing, while others can learn from your experiences.

- **Be prepared:** Just as with insurance, your DP/DR plan might never be put into action but if it ever is, you and your company have greatly increased the odds that you will survive and thrive after a disaster or other data-loss event.

What's in a DR Plan?

Although there is no right or wrong way to document your DR plan, there are certain pieces of information that are vital inclusions for all DR plans. Below are guidelines for the types of details and recovery steps you should include in your written DP/DR recovery plan:

1) Identify the risk(s) are you trying to mitigate with your DP/DR plan

2) Identify how a data loss or disaster could affect company operations.

3) Develop a high-level strategy, including an RTO, for recovering from a disaster or other event, including recovery steps for company phones, website operations, email, order fulfillment, customer service and damaged physical location(s).

4) Document how you will recover and restore data, files, VMs, network connections, access to the Internet and physical servers.

5) Employee recovery activities: Document who will perform which recovery tasks when, including time estimates to complete each task.

6) If your plan includes cold-site recovery, you should have a recovery plan on file with your DR vendor, so that everyone is on the same page in case of a disaster.

7) Include a plan for contingency mode operations. If your SMB loses all computing capabilities, detail what steps can be taken to continue operations in manual mode.

8) Include a test plan to regularly verify that your DP/DR plan will work when needed.

9) Actively review and update your DP/DR plan as your business and computing infrastructure changes.

SSG-NOW
TARGETED ANALYSIS

Outlook Report

Vendor/Product Profile:

SSG-NOW's Take on DP/DR for SMBs

Few technological advances offer as much utility and value to SMBs as does the preponderance of data protection and disaster recovery products and services now on the market. DP/DR vendors are leveraging economies of scale to provide cloud-based DR and DP services for SMBs that prior to now might not have been able to afford either. With DP protection costing less than $10 per month per computer and offering the ability to access backed-up files from any web browser or smartphone in the world, we consider cloud-based DP to be the new minimum level of protection for an SMB's digital assets. There is simple no excuse for any SMB to not have data protection in place for business-critical data and files.

For SMBs who have regulatory, tax or business drivers requiring a full-scale disaster recovery and data retention plan to be in place, cloud-based DR offers both low-cost DR services and on-demand testing of the DR failover plan. Cloud-based DR vendors offer continuous snapshots of VM images as well as bare-metal recovery capabilities for physical servers. As competition increases in the DP/DR for SMB space, supply and demand puts downward pressure on the cost of DP/DR services. This means that not only are current prices very reasonable and in-reach for most SMBs, but future prices should remain relatively stable--or perhaps go even lower--as the technology continues to mature. We are bullish on both the DP/DR market for SMBs and the ability of most SMBs to take advantage of cloud-based data protection, as well as on-premises DP/DR solutions that seamlessly integrate with a cloud-based backend.

Never before have so many SMBs been able to acquire sophisticated DR and DP capabilities for such a reasonable cost. Consider what a complete failure of your computing infrastructure would cost your SMB and you will discover that the cost to recover from just one data loss event per year will more than cover the cost DR and DP protection to begin with. The ability to take continuous snapshots of your VMs and the ability to test the disaster recovery process with the click of a mouse is not just cool, it is revolutionary at this price point. We strongly recommend that all SMBs reading this paper consider investing in a DR and/or DP service that protects them from disasters and other data loss events.