MAXBackup™

MAX INSIGHT

Whitepaper

4 Business Continuity Best Practices Every MSP Should Follow

By Jay McCall

We are Max

MAXfocus™

Table of Contents

Executive Summary

Banking on traditional backup and recovery methods to protect your customers' data could leave you and your customer with an unexpected surprise in the event of a server failure – with all fingers pointing to you.

In this whitepaper, we'll explore four best practices MSPs and IT service providers should follow to ensure they're providing customers with the best business continuity and disaster recovery (BCDR) solutions and services possible, and maximizing their recurring revenue potential at the same time.

In addition to sharing business strategy tips, we'll explore the increasingly important role that MAX Backup's Virtual Disaster Recovery (VDR) service plays in creating a solid BCDR strategy.

The Real Cost of Downtime

As a VAR or MSP, your customers need you to be much more than the "IT guy" who fixes their computers or networks when something goes wrong. They need a virtual CIO who's able to guide their IT buying decisions and help them make smart business choices. Yet, studies show that when it comes to one of the most important IT decisions — protecting customers' data — many resellers are taking a "wait-and-see approach." A 2013 survey of 350 IT experts conducted by The 2112 Group and *Business Solutions* magazine revealed that 44 percent of technology firms depend on breaches, downtime, and clients raising concerns about unprotected data rather than proactively marketing and selling backup and recovery solutions. Additionally, research from Pricewaterhouse Coopers suggests as many as 96 percent of PCs are not adequately backed up. At least once a year, most small to midsize businesses will experience at least one instance of downtime. While that may seem like no big deal, Aberdeen Group estimates an hour of downtime costs midsize businesses an average of $74,000. A Harris Interactive survey sheds further light on the matter, revealing that IT managers estimate 30 hours on average for recovery time.

So, considering the fact that some unexpected downtime is highly likely to happen to your customer at some point during the next 12 months, and it's very costly for end users to recover from, wouldn't you agree that selling BCDR solutions and services is an important first-step in distinguishing yourself from your competitors? So do we, which is why we've put together the following four tips to ensure that when the inevitable server failure or disaster occurs, you customers' business systems and data will be quickly and easily accessible.

Best Practice #1: Create A "Better Than Tape" Backup Strategy

Although the consumer world has gracefully made the transition from cassette tapes to CDs and now to digital files, many businesses are still stuck in the tape era when it comes to backing up their data. It's not that tape doesn't still have its place in the workplace – it's actually ideal for long-term archives that end users may need to satisfy legal discovery requirements or financial audit requests. However, using tape for backing up day-to-day mission-critical data is not ideal for several reasons, including:

1. Tape backups are often performed manually, which means that missed backups and other human errors are inevitable.

2. Tapes are easy to lose. Most businesses' tape-based disaster recovery plans include having an IT person keep backup tapes at home or in their vehicles, which presents both a security risk and the risk of losing tapes.

3. Have you tried to restore data from tape lately? Not only do you need to have the right device, drivers, application and OS, but the wait alone to retrieve a tape from offsite can easily eat up an entire work day.

4. And here's the crux of the matter: tape backups are notorious for what's known as silent data corruption, an insidious problem that causes data restores to fail – more than 40% of the time according to some sources!

So, the bottom line is this: If you're involved with a data backup and recovery discussion with a client or prospect and they try to indicate they're all set because they back up their data to tape, be prepared to help them self-discover why *not* using a hybrid-cloud backup solution is setting them up for a costly disappointment down the road.

Best Practice #2: Hybrid Cloud Backup Is the Best Business Continuity Policy

Another pitfall some IT service providers fall into with regard to protecting clients' data is keeping only a single copy of a client's data. For example, some may back up their data on-premises to a NAS (network attached storage) appliance or other dedicated backup appliance. That's good, but what happens if the building catches on fire, or it's flooded or destroyed by a disaster? The May 23, 2011 tornadoes that ripped through Joplin, Missouri caused $2.8 million in damage and affected more than 17,000 people. A year later, Hurricane Sandy resulted in approximately $65 billion worth of economic loss among the United States, Canada, the Bahamas, and the Caribbean. In 2013, an EF-5 tornado hit the city of Moore, OK, causing $3.8 billion in damages. Keeping one's data on-site only is clearly risky business. And, when you add the fact that 93 percent of companies that lose their data for 10 days or more due to a disaster file for bankruptcy within the following year (Source: National Archives & Records Administration in Washington) , backing up your customers' data off-site becomes a no-brainer.

Although the cloud has become a viable source for businesses to store their data – and to run certain business applications – even the best cloud providers can experience occasional outages and sometimes a company's Internet connection to the cloud can fail (e.g. during a storm or if a cable line is accidentally dug up). For these reasons, a hybrid cloud backup strategy is the recommended best practice. The MAX Backup solution supports the hybrid storage approach, enabling partners to back up their customers' data in a secure cloud environment, where customers' data is protected from any worst-case disaster scenario. And, at the same time, the Backup solution allows partners to provide their customers with local VM (virtual machine) image backups that can be quickly spun-up should a client need to recover a file without an available Internet connection.

Best Practice #3: VDR Is a Welcomed Change to Traditional Image- and File-Based Backups

Traditional backups come in two varieties: file-based and image-based. Some backup products perform only file-based backups and others perform only image-based backups. Each type of backup offers specific benefits and drawbacks. For example, an image-based backup captures all your data – files, folders, applications, drivers, and operating system – in a single "snapshot." If a file server crashes, a local image backup is the quickest way to restore your data. However, because of its size, storing these images in the cloud can be very difficult *and* costly. Plus, attempting to restore a system image from the cloud can take several days, which is outside most customers' RTO (recovery time objective) requirements. File-based backups, on the other hand, provide a smaller footprint than system images, and they are much more "cloud friendly." In situations where a file is accidently deleted or becomes corrupted, for example, the most recently saved good version of the file can be retrieved from the cloud in just a few minutes.

For clients with RTO requirements of two hours or less, MSPs and IT service providers used to have to deploy expensive redundant physical servers, incorporating nearly identical specifications to the original (e.g. same RAID configuration, CPU type, operating system, and drivers). In addition to the expense of maintaining redundant servers and managing backup products from multiple vendors, performing a complete image restore could still take several hours.

MAX Backup's VDR solution eliminates the limitations of traditional image-based and file-based backups mentioned above. In this virtualized environment, the business applications and operating system are logically separated from each other, and they're separated from the hardware appliance, which turns these mission-critical business applications and data "images" into the equivalent of files and folders. What's more is that a virtual backup can be restored to *any* hardware appliance — it doesn't have to match the original system.

Some MSPs have the misconception that virtualization is only practical for enterprises with dozens of servers residing in large data centers. Thanks to changes in some of the leading virtualization company's licensing models and the increase in the number of software vendors integrating with these virtual platforms, virtualization is now a viable option for SMB customers, too.

The MAX Backup VDR solution enables channel partners to recover failed physical Windows systems as a VMware or Microsoft Hyper-V compatible virtual machine. With this added functionality, MSPs can:

- Provide remote assistance to perform a virtual recovery at the client's location using the customer's own virtual environment.
- Perform a virtual recovery within the MSP's datacenter using a virtual environment owned by the MSP. The recovered system can then be made available to the customer for a short period of time.
- Perform a virtual recovery to an offline VM and ship it on physical media to the customer or an IaaS (infrastructure as a service) partner.
- Stage a virtual recovery and perform daily incremental restores to keep a near-line copy available for rapid disaster recover (DR) purposes
- Leverage VDR to perform recurring DR testing services for the client
- Leverage VDR as a tool to do a one-time conversion of a client's physical machines into VMs hosted by the MSP

Not only does this new offering enable partners to provide clients with a complete and highly-customized DRaaS (Disaster Recovery as a Service) without the hassle of trying to piecemeal multiple vendors' products, it allows MSPs to boost their recurring revenue and develop stickier customer relationships at the same time.

Best Practice #4: VDR Is the Cure For Silent Data Corruption, Too:

Although silent data corruption is a problem that's primarily associated with tape backups, it can occur with other backup media as well. Additionally, as Internet-borne viruses become increasingly sophisticated and insidious (e.g. CryptoLocker, Storm Worm), corrupted files can be inadvertently backed up. In a traditional physical image backup environment, the only way for the IT service provider and customer to ensure a backup was "good" was to perform a data restore, which required building a duplicate server (expensive) and running an actual restore (time consuming). As one might imagine, this step was often either performed infrequently or skipped altogether. In a VDR environment, where testing can be performed quickly, inexpensively, and without disrupting the primary server environment, nightly data backup testing is now a viable option MSPs and IT service providers can and should be incorporating into their BCDR offerings.

Selling BCDR to clients faced with ever changing industry regulations and a myriad of security threats can be intimidating enough to cause some MSPs and IT service providers to wait for customers to approach them *after* experiencing data loss. Employing a holistic BCDR strategy that incorporates file- and image-based backups using an on-premise and off-premise (i.e. in a secure cloud data center) environments, and using the latest virtualization technology to meet customers' RTO requirements overcomes these fears. Additionally, when MSPs and IT service providers change from reactive selling to proactive business consulting, they move away from commodity-based IT sales and towards the more profitable and rewarding experience of long-term recurring revenue.

For more details visit www.maxfocus.com/backup

USA, Canada, Central and South America

4309 Emperor Blvd, Suite 400, Durham, NC 27703. USA

Europe and United Kingdom

Vision Building, Greenmarket, Dundee, DD1 4QB, UK

Australia and New Zealand

2/148 Greenhill Road, Parkside, SA 5063

www.maxfocus.com/contact

WP0018-v1.0-EN

We are Max

MAXfocus™
From LogicNow