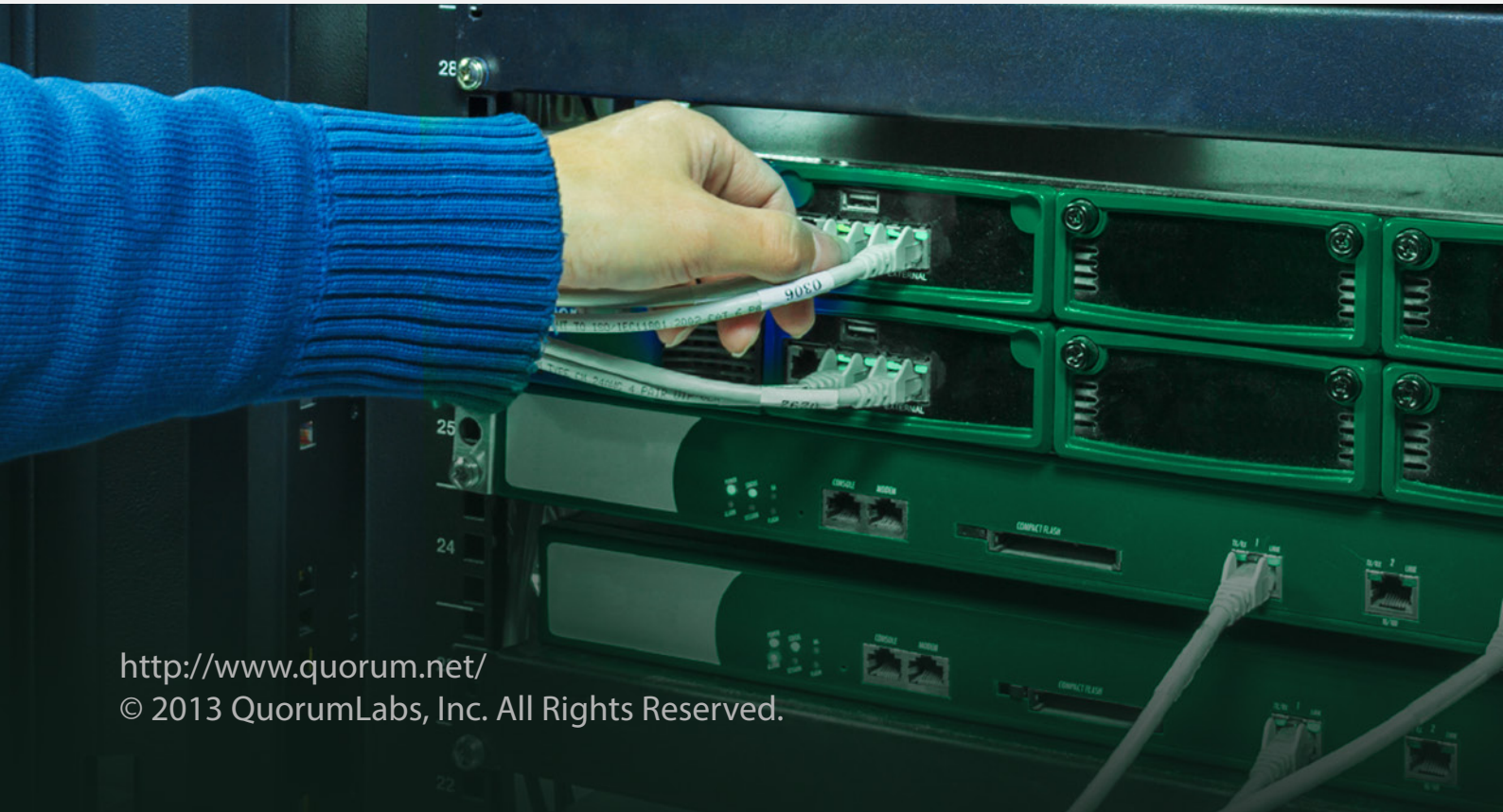
Quorum®

WHITEPAPER

Always Be Testing:

Making the Case for "ABT"

It's time to stop playing Russian roulette with your small to mid-sized business. Make a commitment to "Always Be Testing" ("ABT").



http://www.quorum.net/

Whether caused by a hurricane, a virus or a storage failure, statistics show that most to mind-sized businesses will experience at least one instance of system downtime a year. Once a year doesn't seem like much, but consider this: Aberdeen Group estimates that an hour of downtimes costs a mid-sized business an average of $74,000.Then factor in results from a Harris Interactive Survey, which found that IT managers estimate 30 hours on average for recovery.

Now that the cost has been put into perspective, are you sure your business can back from even one instance of system downtime each year? Has your disaster recovery (DR) system been through regular real-world tests to find out? Unfortunately, only a small minority can respond to this question in the affirmative: A 2011 survey found that only 28 percent of small to mid-sized businesses surveyed have even tested their backup at all.

But even for that 28 percent, texting once or twice a year, quarterly, or even monthly is simply not enough. As you'll discover after reading this report, changes in your environment-whether in hardware, software or in the environment's configuration, for example – make the case for weekly testing mustn't focus solely on a sampling of servers or files. Rather, a full DR test that accounts for every change that was made is the only way to avoid potential problems in the all – important recovery of data, applications and systems.

Testing Has a Bum Rap, But Does It Have To?

Despite the undisputed fact that system downtime is inevitable, many organizations remain steadfast in their outdated belief that DR testing is more trouble than it's worth.

Their four specific complaints:

Testing takes too long.

Testing is too complex an endeavor.

Testing involves too much planning and saps resources.

Testing is too costly.

Of course, if an organization is using tape or disk backup for disaster recovery,these complaints are not altogether unfounded. Testing in tape or disk backup environments,for example, involves the cumbersome job of physically locating and retrieving the tapes/disks that have been sent off-site for safekeeping.

Cloud backup alone has complexities in retrieval as well, with some added costs. The expense of pulling back an entire server's data - let alone an entire enterprise's data -for testing is high, and involves the cloud storage vendor pulling the data, putting it on a USB disk and shipping it.

But performing weekly, real-world tests of your DR system doesn't have to be complex, costly, or a time and resources suck. Your DR solution choice has a lot to do with this. Hybrid cloud solutions, for example, offer on-demand and automatic testing that can be performed in minutes. Once reassured with a weekly test, organizations can feel confident that total recovery is only minutes away should a disaster hit.

But another point to keep in mind is that it's not just the ability to test for data recovery that makes a DR solution valuable. Rather, it's the solution's ability to recover applications and systems as well. Unfortunately, traditional tape and disk backup, or cloud backup alone, can't offer this.

Common Pitfalls Emphasize Importance of Weekly Testing

Many organizations simply aren't aware of everything that can go wrong when recovering emergency backups, and if you never actually try to restore a file, application or server, you don't really know if you can. But because of the aforementioned time and cost issues associated with tape, disk and cloud backup, IT professionals resort to some "workarounds:" They may perform a scaled-down version of a test in either a partial environment or in a partial format. For example, they may test only their organization's Exchange server, but not the SQL server. Or they might take a server down and bring up a virtual copy of it. The problem with these approaches is that testing is not done from "A to Z" on a regular basis, with all data, on all servers, involving all hardware and components, and accounting for all changes in the entire environment. It bears repeating that these changes occur daily.

This brings us to a sampling of some important (but perhaps not obvious) pitfalls that can be avoided with weekly testing, which help identify the molehills before they turn into mountains.

Changes in Hardware, Software, Systems

An organization's infrastructure is constantly changing -if not daily, then weekly. Servers, applications and systems are added, modified and removed, and your backup and recovery system must take these changes into account. A test might be executed on Monday, but by the Monday following, your test is completely out of date, thanks to these changes.

Microsoft's Patch Tuesdays also introduce changes that could spell trouble if regular testing is ignored. These security patches are released once a month, but the company also releases updates on "extraordinary Patch Tuesdays," which fall two weeks after the regular Patch Tuesday. Some updates are even published daily, such as for definitions for Windows Defender and Microsoft Security Essentials. And it doesn't stop with Microsoft: SAP advises users to install security updates on "Security Patch Days," which coincide with Microsoft's Patch Tuesdays. And Adobe Systems' update schedule for its Flash Player joins the fray on Patch Tuesdays as well.

Changes in hardware, too, can be overlooked. When installed, new hardware is tested once. Regular testing after that seems superfluous to many, the argument being that the main DR software hasn't changed, so the test results won't change from the first time. But if any new hardware has been installed (like added storage) or upgraded (such as network cards) and the DR software hasn't been tested on the new platform, cracks can emerge.

Unfortunately, a common practice is to test a tape to ensure the data on it is good, and that files can be recovered. After this type of test, IT professionals have the false sense of security that an entire server can be restored. But if the server itself hasn't been tested regularly, nor the drivers, the RAID controllers or the NICs, there is no way to know that everything will perform as expected when it's needed most.

Backup Corruption/Backups Executed Incorrectly/Human Error

Backup corruption is especially prevalent in tape environments. Tape media spins at a very high speed, and over time, the tape stretches and becomes unusable. Tapes are good for about 20 rotations, but are switched out rarely, if ever. So unfortunately, there's no way to know a tape is corrupt until a data restoration is attempted. Corruption can also occur if a backup device has been damaged or incorrectly processed, or if the storage device has some sort of physical defect. Worse yet is if invalid data has been unknowingly backed up repeatedly over a long period of time. This means all backup copies have been corrupted.

While corruption with disk backup is far more infrequent, it has significant drawbacks that should be mentioned. Organizations are still limited by how much data they can retain for a long time. Disks may be added as needed, but this approach still only allows for backup and recovery, not full DR testing. Chances are, testing is used only to see if a file can be restored, which falsely indicates that the data on an organization's repository is sound. But in this environment, they're still not testing every single file of every single backup.

Human error and flaws in the execution of backups occur very frequently, especially in tape environments. If backups are set up correctly, tapes will be "locked" for a specific amount of time, preventing overriding of data. But if the backup was set up improperly and the tape was somehow not locked, data on that tape will be overridden.

Another example, common among businesses that host their own SQL databases or Exchange servers, highlights a lack of proper backup training. It's an unwelcome surprise when you load up your organization's backup tapes and find that only the flat files have been backed up, and not the database. Even if your IT staff is well-trained, they're still only human, and as such, are prone to human error.

Of course, these issues would be pointed out immediately with weekly tests of an organization's entire environment.

ABT Success

So now that we've stressed some of the perils of not testing (weekly or at all), it's time to present some practical benefits. The following ABT success story is a good start. It emerges amid the destruction and chaos that were the byproducts of Superstorm Sandy.

24 Seven, a New York-based talent and recruiting firm, had just finished testing its hybrid cloud DR solution when Superstorm Sandy hit last October. Thanks to its commitment to ABT, 24 Seven was confident that it could maintain business as usual in the storm's wake without missing a beat. Indeed, the company's downtown Manhattan headquarters had to close, but payroll - 24 Seven's main responsibility - was still performed, ensuring the company's reputation remained intact. Certainly, close calls like this bring perspective to the importance of adopting ABT as part of your overall business continuity plan.

Aside from the obvious benefit of assured recovery, automatic weekly testing (afforded by hybrid cloud solutions) also frees time to focus on the finer, more strategic points of business continuity that are more common among large businesses. For example, IT professionals can engage their employee base

by conducting quarterly "fire drills," ensuring notification emails are sent out correctly, and making sure employees can connect through the VPN so work can continue without interruption even after a disaster.

One thing is for sure: You can never count on your DR system performing 100 percent of the time if you test it 0 percent of the time.

Further, given all the changes or missteps on a network, you must be able to test weekly: Even a tiny change to your IT system increases the odds that something might go wrong later on.

Still not convinced that weekly testing is important? Then ask yourself this question: Would you feel comfortable erasing your hard disk right now, and restoring it from your backups? If not, it's time to commit to a new routine: "Always Be Testing."