The ABC’s of Disaster Recovery Testing

DR testing is a critical part of the business continuity process. It is the only way to ensure you’ll be able to recover data and applications following a disaster. Thankfully, a number of recent technology developments have eased DR testing, making it much more practical for IT teams.
New Techs Ease DR Woes

**Disaster recovery testing** can range from a simple tabletop exercise to a full-scale emergency simulation. And, just as a disaster recovery plan reflects the specific needs of an organization, DR testing also must be tailored. In other words, a DR test of computer systems at a small high school will obviously look a lot different than that of a large hospital. A DR test at a high school in Massachusetts might even be quite different from a test at a high school in another state—because of specific weather threats, local laws, technology budgets and other variables. DR testing may encompass more than technology, but technology will be a component of nearly every DR test.

Our surveys have shown that many IT pros lack confidence in their ability to restore operations in a reasonable amount of time following a disaster. Historically, IT disaster recovery testing has been a difficult process, often requiring application downtime. Because of this, DR tests were conducted infrequently or not at all. Today, this is changing. Advances in technology—particularly server virtualization and cloud computing—are easing the testing process. These technologies allow users to easily set up a test environment minus the large cost of additional hardware. Also, today’s sophisticated DR software can manage the testing process and continuously monitor your environment. If you host DR data with a cloud service provider, testing is often included.

This Drill Down on DR testing offers in-depth information on these technologies, DR testing best practices and advice on how to create DR test scenarios for your environment. If you are getting started with DR planning and testing, or you haven’t run a DR test in a while, we’ve got you covered.

Andrew Burton
*Executive Editor, SearchDisasterRecovery*
Server Virtualization Eases DR Testing Headaches

**Disaster Recovery is** insurance, an infrastructure and a set of processes that a company may rarely use, but it is essential when the time comes.

For it to have value, a disaster recovery plan and infrastructure must be tested. Historically, testing disaster recovery products has been difficult, time-consuming and expensive, so it was often neglected.

However, server virtualization, sophisticated disaster recovery software and cloud computing are making regular DR testing feasible and cost-effective.

**Local DR Testing**

For disasters such as the failure of a single critical server or storage system, recovery means firing up an instance of the application on a secondary server on-site. This requires that a cloned copy of the virtual machine (VM) image has been created on a standby server running the appropriate hypervisor. Some of this can be done using tools native to the virtualization platform, but many companies use specific disaster recovery software for a couple of reasons.

These products can keep the DR copy updated with the primary VM efficiently, using snapshots and replication. Many can also convert a physical server and its applications to a VM as part of the initial cloning process, and then keep it updated as they do primary VM images. Capturing the current state of a production server is not trivial and DR planners must take this into consideration.

Also, it’s critical that before the DR test is run, a clean, quiesced copy of the protected data is captured. While an application can typically be rebuilt from “dirty” data, this will increase the recovery time and may result in some data loss. It’s also important for the
organization to understand that in the event of a real disaster, there will probably be some data loss, unless the application being tested is gracefully shut down. At a minimum, this involves data in transit but more likely includes data added or modified since the last clean update.

When it comes time to test that recovery process, the cloned VM is restarted on the standby server and users are pointed to that VM. If a more complex stack is involved, like Web servers, load balancers or database servers, DR software can actually orchestrate the entire process, starting each application in order and monitoring the environment. Again, this isn’t trivial and care should be taken to understand all the steps involved so they can be included in the test.

**REMOTE DR TESTING**

When the DR location is remote at a secondary site or in the cloud with DR as a service (DRaaS), testing is essentially the same process, but the updated VM images are stored off-site with the compute infrastructure that’s running the hypervisor instead of on a local standby server as described above. Testing involves restarting the replicated VMs and pointing users to them. The real difference is that when these VMs are actually used in a DR situation, network latency will come into play.

The cloud is an increasingly popular DR target, because it offers flexibility and cost-effectiveness that an in-house secondary site does not.

For this reason, a hybrid DR product is an appealing option. Combining the local and remote approaches, a failover server is kept running in the company data center, and is synchronized with another system off-site.

The cloud is an increasingly popular DR target, because it offers flexibility and cost-effectiveness that an in-house secondary site does not. For example, many DRaaS products offer hot, warm and cold DR options at different price points. Depending on the RTO of a particular application, users can choose the
right approach for their organization’s needs and budget.

Historically, disaster recovery testing for most companies has been a less-than-comprehensive process conducted on a less-than-regular basis, which has often eroded the confidence in the DR system, at least among those who knew the details. But now, mostly due to the emergence of server virtualization, DR testing can be a much simpler exercise that’s not just limited to nights and weekends. The result is a DR system that can provide the peace of mind that a good insurance policy is supposed to. —Eric Slack
DR Testing Still Required, Even in the Cloud

A disaster recovery test can reveal issues with the mechanisms put in place to restore your organization’s IT operations following an outage. Will the system work as planned? Are you able to bring systems back online to meet recovery time objectives and recovery point objectives? The issue becomes murkier if you turn to a third party to handle disaster recovery operations for you—who is responsible for what process, and how can your organization be sure it will get what it pays for? In this Q&A, Jason Buffington, a senior analyst at ESG, discusses some best practices when it comes to DR testing.

How often should you test?
I would not expect someone to do a full-scale DR test any more frequently than six to 12 months, and that’s based on the criticality of the data and the industry that they are in. However, even though you won’t full-scale test, the idea of randomly picking a server or a core application on a monthly basis ... and on a recurring basis, [is a good one]. Test something different, a small component of the plan. That coupled with an annual full-scale test will ensure most pieces and parts are covered. What a lot of people don’t understand is that the resiliency that you get in business continuity planning and recovery preparation also yields operational benefits year-round.

How do you determine what you should be testing?
It’s OK to take an honest and authentic look at your infrastructure and say, “There’s maybe 30, 40% of these servers and applications that we really need to make sure we have an additional measure of effort to ensure resiliency for.” So, whatever percentage of your infrastructure you believe requires less than, say, a three-day recovery window, let’s label that “important.”
That stuff deserves an extra level of resiliency and preparation and should be part of the test plan.

**How is DR testing easier today than it was in the past?**

Buffington: recovery exercise is the initial standup of infrastructure. Server virtualization makes all that portable. I don’t have to rebuild physical servers; I can move VMs or copy VMs. So because of that, the testing process is much more straightforward. For some folks, it may be as simple as having a copy of those VMs [virtual machines] someplace else, isolating them and then powering them up. It really doesn’t have to be that hard.

Some backup solutions even come with automated validity check, to make sure VMs are recoverable. Some of those solutions give you the ability to sandbox a set of VMs. You can bring them up in an isolated silo from everything else, make sure they work and power them all down again.

BC/DR is often presumed to be so complex and so expensive that most people aren’t willing to try it. And the reality is, with virtualization and the robust backup and replication tools that are in the market today, BC/DR is viable and obtainable for medium-sized organizations and enterprises. You just have to stop presuming it’s hard.

**Has the cloud made DR easier?**

Using the cloud as an infrastructure stack is one of the best things that an organization can do, because one of the challenges of BC/DR is that you need a second site. And medium-sized organizations often don’t. Even enterprises have to justify how much money they want to put into maintaining a second infrastructure.

So the idea of an elastic, cloud-based infrastructure that costs you pennies when you’re not using it, and is ready to go when you need it, is a godsend. However, from an expertise and a personnel perspective, the cloud is not a silver bullet, because most cloud providers do not have BC/DR expertise to help you get back up and running as quickly as your business demands. Also, no one cares as much about your organization’s ability to restore service as you do. People shouldn’t think they can just
write a check on a monthly basis and not worry about it anymore. Organizations still need to own their own BC/DR plan. A cloud provider may be able to supplement your expertise, but your recovery plan is your recovery plan.

Do testing measures vary among cloud DR providers?
One of the things you should look for is that a lot of data protection service providers [have] a wide range of features. They charge you next to nothing to push your data into their cloud, and they want to charge you inordinately on the way back out.

Depending on the model, you might be incurring quite a bit of recovery costs and sticker shock afterwards. You want to be sure that the service provider you choose supports the idea that you’ll annually test your plan and routinely test specific parts of the plan. You need to make sure that your data protection service provider has an economic model that doesn’t hinder you from doing the responsible thing of testing.

So, with cloud DR testing, it’s less about ease, and more that other concerns are at play?
When it comes to BC/DR, you still own the plan. If you’re efficient with your IT deployment models, then you can probably do it yourself at a secondary [site] or one of your existing sites. The question is does your IT team and your executive team have the appetite for maintaining that second infrastructure? Or would they rather offload the secondary site to the cloud? It’s really about the culture of your IT team, it’s about how distributed your workforce is ... it’s not economics; you can’t write a check and have the problem go away.

—John Hilliard
Developing Technology Scenarios for BC/DR Exercise Planning

Perhaps the easiest kind of disaster simulation is one that affects technology. However, an event that makes data unavailable can be devastating to many business’ operations. As such, disaster recovery (DR) testing for essential technology should be considered a critical part of any disaster recovery plan. Don’t be content to look at a failed server scenario in your business continuity (BC)/DR exercise planning; tests should be more ambitious, like an accidental release of overhead sprinklers in the equipment room that damages multiple devices, many of which are running critical applications and processing protected data.

Another possibility would be to consider a networking scenario in your DR exercise planning, as it could have a farther-reaching impact on multiple company locations, which in itself makes for a more interesting challenge. A distributed denial-of-service (DDoS) attack can work, as it affects multiple locations—each of which may be running mission-critical systems.

Introduce the element of a timed sequence of attacks occurring over a four-hour period to your disaster recovery (DR) exercise planning process. Just when one incident appears to be addressed, another, far worse, attack occurs. Given the pervasive nature of technology today, almost anything is possible in terms of a potentially destructive incident.

These BC/DR exercise planning scenarios focus on disruptions that affect systems, networks, and software, data, and support infrastructures.

Scenario: Server failure due to improper maintenance and installation of untested circuit board.

Description: Despite all normal precautions, server outages do occur, and may happen for reasons other than a failed circuit board or
power loss.

**Why Use It:** This is a key scenario for technology disaster recovery plans, because servers handle so many different functions.

**Scenario:** Malfunctioning network router causes cascading outage across a large multi-point network.

**Description:** Today’s networks are so densely interconnected that any errant code could bring down an entire network.

**Why Use It:** All elements in a network—whether voice or data—must be regularly tested to ensure they are performing properly.

**Scenario:** Software glitch introduced in IP signaling network causes network disruption.

**Description:** Such an event occurred in AT&T’s network back in 1991; such a threat is always possible, despite improved network software.

**Why Use It:** This is a fairly severe example, but a private voice/data network could be compromised by damaging the signaling infrastructure.

**Scenario:** Failure of SAN infrastructure results in inability to back up critical data.

**Description:** Loss of SAN technology could make it very difficult to perform daily backups as well as emergency DR backups.

**Why Use It:** Many medium to large organizations link their storage assets via SANs, so this scenario should be considered.

**Scenario:** DDoS attack shuts down global network.

**Description:** Despite numerous available network security safeguards, a DDOS attack could still occur, threatening a firm’s operations.

**Why Use It:** Network perimeter security is a key business requirement, considering that most firms connect to the Internet.

**Scenario:** Burst water pipe located above a server area damages multiple critical servers.

**Description:** Proper location of electronic device areas is very important; planners must examine the infrastructure both above a prospective equipment room and below it for possible threats and vulnerabilities.

**Why Use It:** This is an often overlooked activity that could result in serious and unplanned outages. —**Paul Kirvan**
SERVER VIRTUALIZATION EASES DR TESTING HEADACHES
DR TESTING STILL REQUIRED, EVEN IN THE CLOUD
DEVELOPING TECHNOLOGY SCENARIOS FOR BC/DR EXERCISE PLANNING

JOHN HILLIARD is a contributor to Storage Media Group.

PAUL KIRVAN, CISA, FBCI, works as an independent business continuity consultant and auditor, and is secretary of the U.S. chapter of the Business Continuity Institute and member of the BCI Global Membership Council. Email him at pkirvan@msn.com.

ERIC SLACK is a senior analyst at Storage Switzerland, an IT analyst firm focused on storage and virtualization. Email him at eslack@storage-switzerland.com.

The ABC’s of Disaster Recovery Testing is a SearchDisasterRecovery.com e-publication.

Rich Castagna | VP of Editorial/Storage Media Group
Ellen O’Brien | Associate Editorial Director
Andrew Burton | Executive Editor
Ed Hannan | Senior Managing Editor
Dave Raffo | Senior News Director
Linda Koury | Director of Online Design
Neva Maniscalco | Graphic Designer
Jillian Coffin | Publisher
jcoffin@techtarget.com
TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

© 2015 TechTarget Inc. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher. TechTarget reprints are available through The YGS Group.
About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.