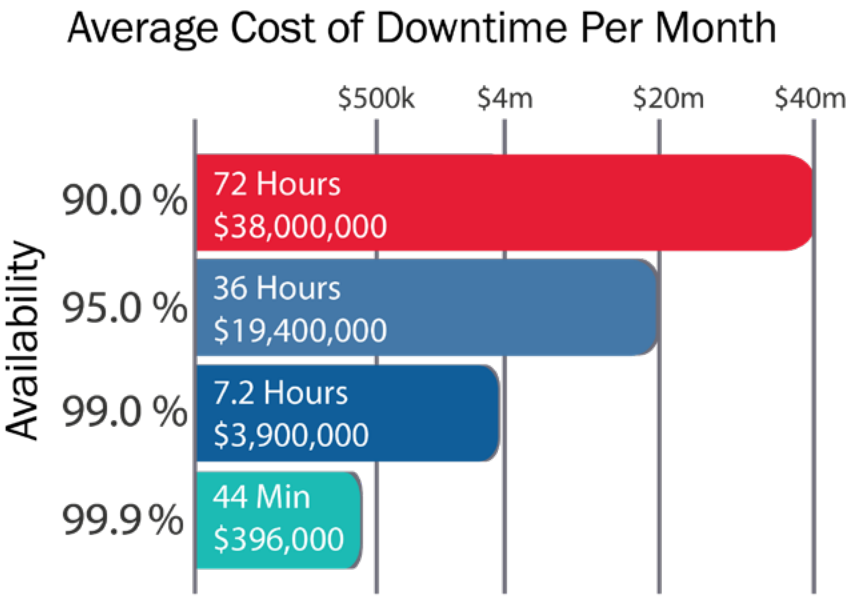
UNITRENDS

DISASTER RECOVERY TESTING, YOUR EXCUSES, AND HOW TO WIN

INTRODUCTION

You can plan, look at diagrams, listen to consultants, but you still won't know that all your recovery capabilities will actually work without testing. Why – because recovery can be complicated. So many things can go wrong – network configurations do not get replicated properly, application dependencies are not in sync across sites, DR resources may become insufficient over time, etc. And the worst time to identify an issue is during an actual emergency.

The cost of failure is high. Failing to recover or deflect attacks results in application downtime. While the cost application downtime varies dramatically across industries, an average for all organizations is about $9,000 per minute in decreased productivity, lost revenue, and other negative business impacts per The Ponemon Institute[1]. While 99.9% uptime is great, shortening that to 99.99% could save an organization about $350,000 per month[1]. This level of uptime is only possible if data protection and recovery solutions are tested regularly, and correction of issues that may slow recovery.



But how often should you test your DR and what tools should you use?

The only way you know you're not wasting time and money on an expensive recovery plan is to test it regularly and see the results. Period.

CURRENT STATE OF TESTING

In our annual survey of the backup and recovery practices of medium to large enterprises, we asked respondents how often they test their recovery capabilities.

The majority of responding organizations reported **testing their DR plans only once per year, less, or not at all**. A lot of changes occur in enterprise data centers over the course of a year. In addition, most industry governing bodies require companies to have business continuity plans and know and document their results. With the pressure to keep businesses up and running, why is testing performed so infrequently?

WHY TEST?

Let's step back a second and make sure everyone agrees that regularly testing recovery is the right thing to do. What does testing provide?

Confidence

Documenting and maintaining a recovery plan is now an essential task of the IT department. You need to prove to senior management that you have a verifiable process in place to recover business services. You need confidence that your business can run in an emergency and documentation that proves it.

Identification of recovery issues

A good testing process will identify issues that impact recovery. These can then be addressed prior to a real emergency.

Compliance reporting

Most companies have industry mandates that require protection against loss of data and functionality. Health care organizations, for example have HIPAA mandates that require not only DR protection, but also that recovery technologies are tested regularly so auditors can see the results.

SOX (Sarbanes - Oxley)

SOX compliance is required by all publicly traded companies. In addition to requiring corporate officers to take greater responsibility for the accuracy of

financial reports, SOX mandates that organizations understand the risks that may impact the financial reporting process. A proper assessment of this risk should include IT risks resulting from inadequate disaster recovery or business continuity plans.

Job Security
Failing to raise the criticality of testing can leave the business exposed in ways that can limit the careers of IT professionals.

IT professionals are intelligent. If testing is so important why don't companies test more often?

The reason is testing can be costly, difficult and risks interrupting critical business processes.

EXCUSES ORGANIZATIONS USE FOR NOT TESTING MORE FREQUENTLY

When polled, most organizations cite several reasons why they don't test more often:

Testing takes time
IT pros are already overwhelmed with the day to day tasks of managing complex and extensive IT infrastructure.

Testing can disrupt production systems
Many test procedures require that you bring down production in order to validate the test. And if traditional restore processes are used, this downtime process can be very impactful. So much so, that organizations feel the need to cut corners in the process, which leads to false positives, high risk, and wasted time.

Testing can cost money
Outside providers are playing an increasing role in providing disaster recovery services. DR testing can create charges for things like public cloud compute cycles, 3rd party recovery services, or consultants that have to be included in an IT budget.

Undocumented DR plan
While most organizations will claim to have a documented DR plan, most are not regularly updated, dependent on a

While most organizations will claim to have a documented DR plan, most are not regularly updated.

Vendors of backup and recovery technology may support only lower levels of testing, yet claim they have full testing capabilities.

few key individuals, on a spreadsheet or Word Doc, and are difficult to locate. Testing will more than likely create the need to update the plan, requiring more time be spent on something everyone hopes will never be used.

LEVELS OF TESTING

There are many different ways to test data backup and disaster recovery capabilities. Some are very basic and check only that data has been replicated to the right location. Others actually test functionality to ensure users can perform their jobs. Vendors of backup and recovery technology may support only lower levels of testing, yet claim they have full testing capabilities, so research is required to determine exactly what they support. Examples of the different levels (basic to advanced) are:

Data verification
This test just checks that blocks / files are good after they have been backed up. Needless to say this level of testing does nothing to ensure the applications can be functionally recovered.

Database mounting
Verifies a database has basic functionality within backups.

Single machine boot verification
Verifies that a single server can be rebooted after a downtime event.

- Single machine boot with screenshot verification – this test goes a little past boot verification by sending an image of the operating system splash screen to administrators as proof the system can be recovered.

DR Runbook testing
Multiple machines are spun up for testing. This is especially important for multiple servers that deliver a business service together, such as an ERP system or clustered databases.

Recovery Assurance
This is the highest level of testing as it includes multiple machines, deep application testing, SLA assessment, and analytics as to the reason any recovery failed.

Anything other than Recovery Assurance still leaves questions about a full recovery. For example, booting to the splash screen may indicate that the operating system can boot, but it proves nothing about its functionality and responsiveness to the business.

You should also consider outsourcing your DR program to professionals. Disaster Recovery-as-a-Service providers embed testing as part of their offering with the best performing full recovery assurance testing. Traditional DR in the public cloud does not include this and can lead to organizations spending thousands of dollars per month with no idea if they are gaining any business value. Look for DRaaS providers that offer recovery Service Level Agreements (SLAs) as effective testing is the only way they can ensure they are not paying large amounts for non-performance.

THOSE OLD EXCUSES FOR NOT TESTING ARE NO LONGER VALID

Fortunately there are cost-effective, intelligent technologies available that can automate, orchestrate and analyze application recoverability to ensure entire workloads are functional and, if not, report what is broken. Additionally, you get an easy to read, formal report certifying the final results of a DR test that can be shared with auditors and senior management. These tools automate testing so you know exactly how fast and to what point your data and applications are protected without requiring much manual work or extra expense. The excuses for not testing are no longer valid:

Testing Takes Time

No more, **it is fully automated**. The results are emailed to you for a simple review to see that everything was successful.

Testing can disrupt production systems

No more, **testing can be conducted within isolated labs** that shield production applications from network conflicts. They can be run in alternate locations, such as cloud infrastructure.

Disaster Recovery-as-a-Service providers embed testing as part of their offering with the best performing full recovery assurance testing.

Tools automate testing so you know exactly how fast and to what point your data and applications are protected without requiring much manual work or extra expense.

Additionally, they often do not even require additional storage given that test can be run against your backups.

Testing can cost money

While testing will never be totally "free", focus on the TCO with the payoff being business continuity and data protection.

Undocumented DR plan

DR Specialists can **help develop your DR plan and new web tools can keep it readily available to everyone on the team**. In addition Recovery Assurance can document its DR recovery steps as part of its runbook setup.

Also, all of these excuses can be overcome by outsourcing your recovery program to experts. They will do all recovery testing and take on the business risk of slow recoveries with SLAs that payout for RTOs that do not meet the contracted goals.

NEXT GENERATION TECHNOLOGY

These next generation technologies can automate testing and reporting to give 100% confidence that recovery can and will take place as required.

Recovery Assurance

Recovery Assurance delivers fully automated recovery testing. Running either locally on the backup appliance or in the cloud, Recovery Assurance will automatically test and certify full business service recovery. Using backups, the entire infrastructure is recreated and booted up to ensure that all data and application dependencies are correct.

Recovery Assurance can be directed to use as many of 50+ built-in tests that are appropriate for your environment. These can include:

- Running and verifying a database query,
- Mailbox transport submissions on Exchange
- Validating service availability, and
- Build and run your own custom scripts to test unique aspects of your workloads.

Unitrends Recovery Assurance verifies the success of each point in time that an application is protected. It includes built-in analytics that assess the impact of an outage in terms of its projected downtime and data loss. It also reports the results of recovery testing to business stakeholders (no setup required) in the form of actual RTO and RPO achieved and flags warnings against their goals.

Copy Data Management

Backups are not just for recovery anymore. There many corporate benefits that can be derived from backup files. Copy Data Management (CDM) is a concept that, on command spins up test / dev environments identical to the production servers because they use the latest backups. The technology makes your latest data, applications, and lab environments available instantly for testing purposes. One use case is that organizations can use these sand boxes to identify issues with new software by testing them prior to deployment on production servers. Other uses can be for compliance testing, reporting, and any other purpose that requires fast, temporary access to cloned environments without over utilizing production resources. Once all testing is finished the entire test environment can easily be torn down.

BCDR (Business Continuity & Disaster Recovery) Link

A well documented DR plan is critical to the testing process. Organizations have typically created disaster recovery plans in Excel or Word that are then filed away and dusted off rarely. These can be hard to manage, store, and and have limited access to those who need it. BCDR Link https://bcdrlink.com is a free online tool that helps you build and customize a DR plan. The template follows the most up-to-date guidelines of International Organization of Standardization (ISO) standard 22301 that specifies security requirements for disaster recovery preparedness and business continuity management systems (BCMS) and includes all steps necessary for a comprehensive recovery plan. The advantage of on line access is that everyone knows where it is stored and the author can control who has access.

All testing excuses can be overcome by outsourcing your recovery program to experts.

The amount and frequency of testing should match the critical nature of the system.

Outsourcing to DR Professionals

DRaaS has greatly evolved from its first iterations. World-class DRaaS providers now offer "White Glove" services that free enterprise IT from having to learn, manage and deploy recoveries. DRaaS White Glove providers will do complete DR planning, including setting up the server reboot order so business-critical applications are the first to recover. Recovery is initiated by a simple phone call with the service provider doing all the work. And the best part is that DRaaS White Glove providers offer both 1-hour and 24-hour Service Level Agreements (SLAs) for application recovery with financial recourse for any delays. This high-touch version of DRaaS can be managed and deployed from any location and protect remote sites around the world

SO, HOW OFTEN SHOULD YOU TEST?

So if you have the latest technology, how often should you test recovery? A quick Google search for "How often should you test your DR" shows most vendors and analysts won't give detailed advice. They mostly agree however that enterprises today don't test enough – but even that advice assumes that there is a definition of "enough."

Gartner, in their report "Modify Your Backup / Recovery Plan to Improve Data Management and Reduce Cost" (February, 2017) advises "Perform data recovery testing at least once a year on a subset of data to ensure the backup strategy effectively meets the stated SLA projections." This advice reflects the old world of testing and not the new reality.

The real answer is "It depends"

The real answer is the amount of testing should match the critical nature of the system. Prioritize testing based on the criticality of business services and work your way back to the infrastructure that supports them. If you have machines that require high responsiveness, validate this in your testing. Don't assume that performance is sufficient. Leverage technologies such as replicas vs. backups for highly transactional machines, and include performance scripts to validate responsiveness.

While testing is not free, it is

far easier and more cost-effective than ever. It takes some resources for spin-up, but in many cases those are already available or can be supplemented by using backup storage given modern technologies. You should test as frequently as you can based on your available resources and recovery point objectives. Remember, every recovery time objective that is untested is a risk to your RPOs and can increase the amount of data lost in an outage because you weren't able to verify that a recovery point was successful.

Users of next generation technology can do frequent testing of their entire infrastructure to greatly reduce the risk of recovery. If this is the case you should be testing automatically at least monthly and on-demand after changes are made to the infrastructure! Remember, IT infrastructures are not static environments. They constantly change. Adding new applications, virtualizing new servers, upgrading software, and moving assets to the cloud can break elements of your DR plan, so retest after infrastructure changes are made. If changes are made frequently, you want frequent testing. If changes are not made frequently and data change rates are not high, you can potentially live with less frequent testing.

Testing is so important that you should include this metric in any DR solution purchase. To ensure faster recoveries and lower impacts from downtime choose a solution with automated, free recovery assurance as part of its offering. Or better yet, outsource your DR program to certified experts that will guarantee their performance with SLA's.

1.Average Cost of Downtime - $9,000 per minute Source: Ponemon Institute© Research Report