

Disaster Recovery Preparedness Benchmark Survey

The State of Global Disaster Recovery Preparedness

ANNUAL REPORT 2014

The Disaster Recovery Preparedness Council publishes this annual report to provide an overview of the current state of disaster recovery preparedness for organizations worldwide. It contains the results of a ground-breaking online survey along with recommendations for improving disaster recovery preparedness based on best practices.



Executive Summary

This report presents Disaster Recovery preparedness benchmark trends for a mix of companies from across the globe, large and small, that have taken the groundbreaking Disaster Recovery Preparedness Benchmark Survey this past year. It incorporates a summary of the responses from the DR Preparedness online survey along with recommendations designed to help organizations improve their own DR plans and preparedness.

The bad news: 3 in 4 companies at risk, failing to prepare for Disaster Recovery

Launched in July 2014, benchmark survey results demonstrate an enormous shortfall in DR preparedness of companies worldwide. Using a common grading system from A (the best) to F (the worst) 73% of survey participants or nearly 3 out of 4 companies worldwide are failing in terms of disaster readiness, scoring ratings of either a D or F grade. Only 27% scored an A, B or C passing grade, with the remaining 73% of respondents at risk.

The incidence and costs of outages remains a major challenge for many organizations:

- More than one-third (36%) of organizations lost one or more critical applications, VMs, or critical data files for hours at a time over the past year, while nearly one in five companies have lost one or more critical applications over a period of days.
- Even more alarming, one in four respondents said that they had lost most or all of a datacenter for hours or even days!
- Reported losses from outages ranged from a few thousand dollars to millions of dollars with nearly 20% indicating losses of more than \$50,000 to over \$5 million.

The culprits in causing these kind of losses can be summarized in a lack of disaster recovery planning, testing and resources.

- More than 60% of those who took the survey do not have a fully documented DR plan and another 40% admitted that the DR plan they currently have did not prove very useful when it was called on to respond to their worst disaster recovery event or scenario.
- One third of all organizations participating in the survey test their DR plans only once or twice a year and fully 23% or one in four never test their DR plans. Without testing and verification of DR plans, most companies have no idea as to whether they can fully recover their IT systems in the event of a disaster or an extended outage.
- When companies do test their DR plans, the results are most disturbing. More than 65% do not pass their own tests!



The good news: we are starting to identify DR best practices

Despite the dismal state of disaster recovery preparedness for most companies, there are organizations that scored A and B grades in the benchmark survey. This report examines some of their “best practices” to describe how others might adapt their own DR plans (or lack of planning) in order to become better prepared.

For example:

- More prepared organizations implement more detailed DR plans
- More prepared organizations set specific DR metrics for RTO's and RPO's.
- More prepared organizations test DR plans much more frequently

How you can improve your DR preparedness

Based on the benchmark survey results, the DR Preparedness Council recommends that organizations consider implementing several steps to help ensure business continuity regardless of industry or evolving threats.

1. Build a DR plan for everything you need to recover, including applications, networks and document repositories, business services such as the entire order processing system, or even your entire site in the event of an outage or disaster.
2. Define Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO) for critical applications. Without these important metrics, you cannot set proper expectations and assumptions from management, employees, and customers about your DR capabilities and how to improve them.
3. Test critical applications frequently to validate they will recover within RTOs/RPOs. For DR preparedness to improve, companies must begin to automate these processes to overcome the high cost in time and money of verifying and testing their DR plans.

As both intentional and accidental threats to IT systems continue to grow and accelerate, the DR Preparedness Council is dedicated to increasing awareness of the need for DR preparedness. At the same time, the council seeks to identify and share best practices that can help organizations worldwide feel more secure and confident about their own ability to recover systems when outages and disasters strike.

Company IT management is encouraged to take the survey at www.drbenchmark.org. Participants receive immediate feedback in the form of a DR Preparedness grade from A through F, and a follow up email to benchmark their responses compared with all others who have participated in the survey.

Disaster Recovery Preparedness Council
January 2014

NOTE: The IT Disaster Recovery Benchmark is intended for organizations that have virtualized some or all of their critical applications through the use of a hypervisor such as VMware, XenServer, Hyper-V, RedHat/KVM, or Oracle.



TABLE OF CONTENTS

Part 1 - Where most organizations fail

How Organizations Deploy DR	5
Outage/Data Loss Costs	6
Outage/Data Loss Causes	9
Lack of comprehensive DR planning	10
Lack of DR testing	12
Lack of DR skills and resources	13

Part 2 – Best practices of better prepared organizations

More prepared organizations make better DR plans	15
More prepared organizations set specific DR metrics	15
More prepared organizations test DR plans more frequently	16
More prepared organizations are more adequately funded	16

Part 3 - What you can do to improve your DR preparedness

Build a DR plan for everything you need to recover	16
Define RTO's & RPO's for critical applications	17
Test critical apps frequently to validate recovery	17
Benchmark your DR preparedness with the survey	17
About the survey	18
About the DR Preparedness Council	20

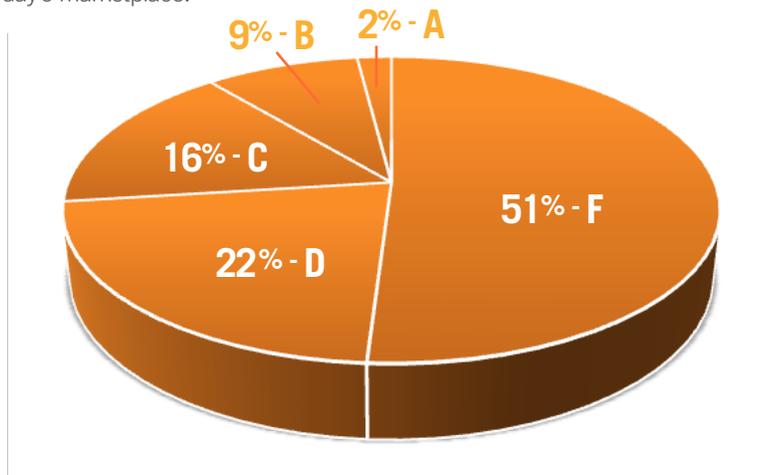


Part 1

Where Most Organizations Fail

3 out of 4 fail to make the grade for Disaster Recovery Preparedness

Based on hundreds of responses and results of the online Disaster Recovery Preparedness Survey at www.drbenchmark.org, most companies worldwide are putting their business operations at risk by not being properly prepared to recover IT systems in the event of a disaster. The survey results indicate a significant gap in disaster recovery preparedness that does not bode well for businesses that typically depend on their IT systems to survive and thrive in today's marketplace.



Nearly 3 out of 4 organizations are at risk of failing to recover from Disaster/Outage

- 51% - F
- 22% - D
- 16% - C
- 9% - B
- 2% - A

According to the survey's results, the vast majority of companies of all sizes are not prepared to recover critical IT systems in the event of a serious outage or disaster. As a result, outages of critical systems are costing business significant amounts of money in terms of lost business, damaged reputations and diversion of resources to remedy and recover from outages or disasters.

Given the general lack of DR preparedness, it is not surprising that nearly two thirds of respondents (60%) said their DR planning and testing did not prove useful in their worst event. The disturbing fact is that most organizations participating in the survey have not documented their DR plans, and have not established key metrics such as RTO, RPO, failover, fallback processes.



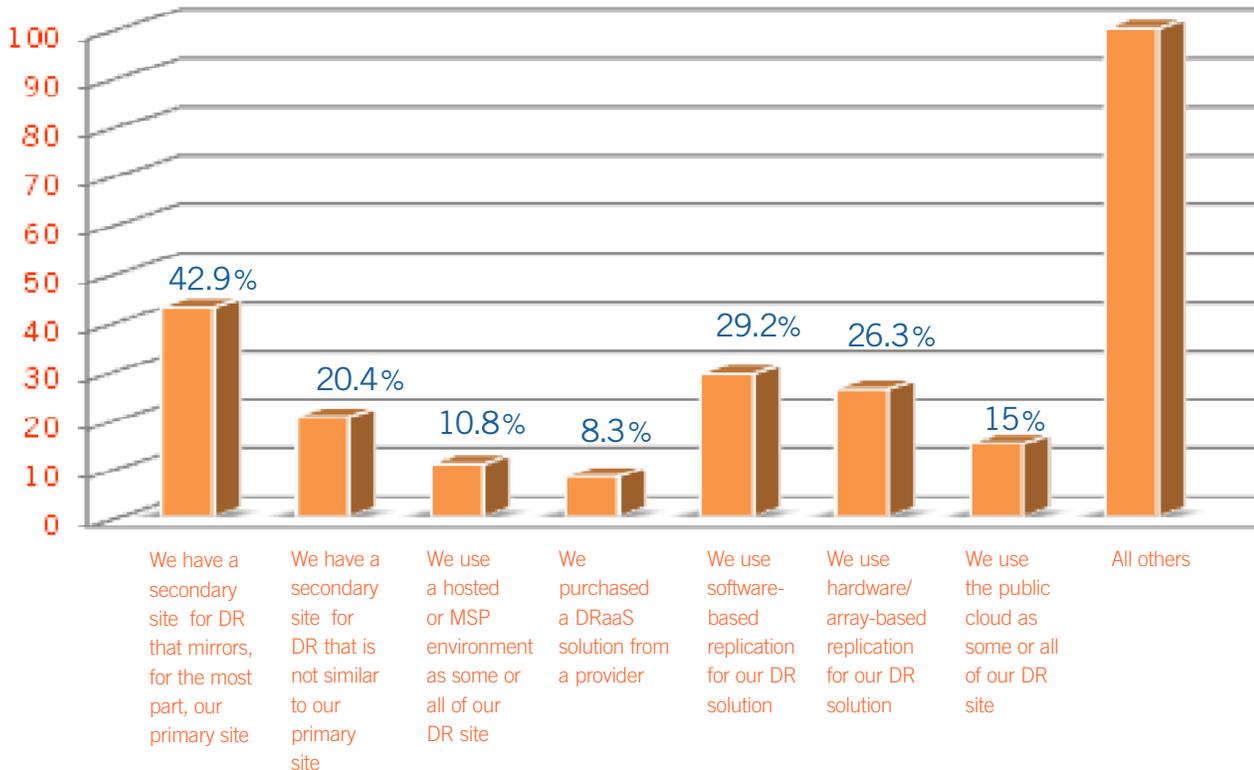
Staff roles and responsibilities are typically not defined well and the majority simply do not test their DR plans often enough to feel confident they can recover critical information and applications rapidly and reliably. And, it appears even more remarkable that one-third (35%) of companies admit to never fully recovering data lost through an outage.

How Organizations Deploy DR

The majority of organizations participating in the survey have made the investment in deploying a secondary site to help manage disaster recovery. About half of organizations use a secondary site that mirrors their primary site, for disaster recovery purposes. Another 20% rely on a secondary site for DR that does not mirror the primary site. While analysts are predicting DR as a Service (DRaaS) will experience explosive growth in the next few years, less than one in ten depend on DRaaS for recovery, and another, approximately 11%, use a Service Provider (SP) or hosted provider for their secondary DR site.

However, a majority of organizations are planning or revising their DR implementation strategies suggesting that 2014 could be a banner year for DRaaS since in many cases respondents lack the internal resources and skills to manage DR implementation and testing.

FIGURE 1
DR implementation strategy dominated by secondary sites





Outage/Data Loss Costs

In an era when an “always available” online presence requires 100% uptime, respondents were candid about the consequences of service interruptions and outages, especially with regard to how much downtime they actually experienced for critical applications and unrecoverable data and backups.

More than half have lost critical applications or datacenter for hours or even days

The survey indicated that more than one third or 36% of organizations have lost one or more critical applications, VMs, or critical data files for hours at a time over the past year, while nearly one in five companies have lost one or more critical applications over a period of days.

Even more alarming is that one in four respondents said that they had lost most or all of a datacenter for hours or even days—an indication of a true disaster scenario for companies that rely on IT to conduct business.

FIGURE 2
Loss of critical data from outages

	FOR HOURS	FOR DAYS	FOR WEEKS	PERMANENTLY	NEVER EXPERIENCED THIS LOSS
Lost one critical application	35.0%	11.7%	4.6%	1.3%	23.8%
Lost multiple critical applications	24.3%	6.7%	2.9%	1.7%	38.5%
Lost most or all of data center	18.8%	5.9%	3.8%	2.1%	43.5%
Replicas not recoverable	12.1%	7.5%	2.5%	2.5%	44.4%

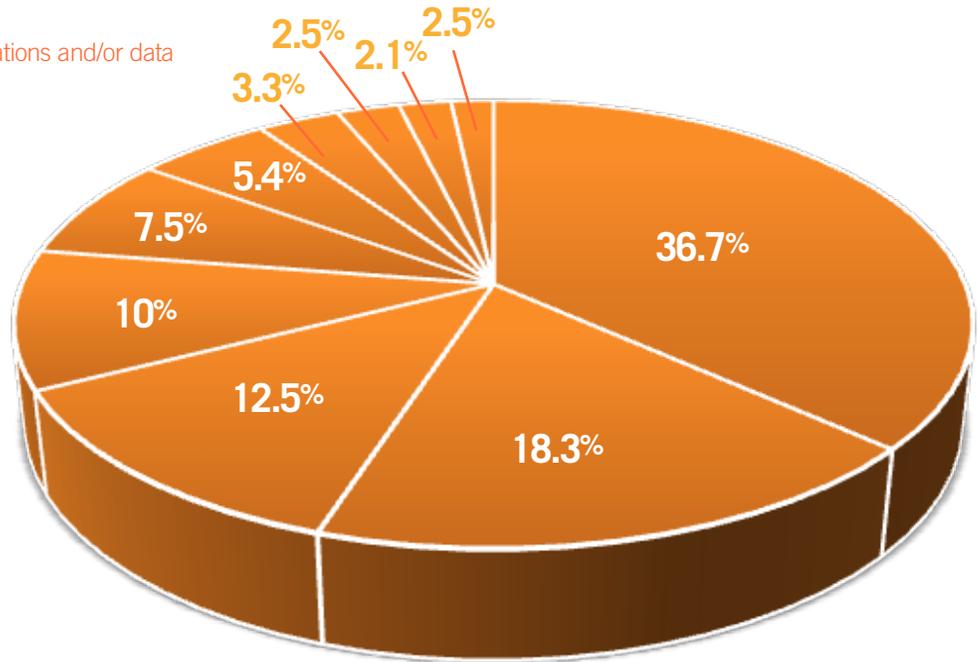


Just as important, in many cases organizations found that the backups and replicas of data were not recoverable after an outage. When an outage occurred and admins were trying to restore from backup and replicas, fully 43%, or almost half, indicated that they were not recoverable.

System outages costing up to millions of dollars

The cost of losing critical applications has been estimated by experts at more than \$5,000 per minute, and our survey respondents confirmed that losses are substantial in some cases. Reported losses from outages ranged from a few thousand dollars to millions of dollars with nearly 20% indicating losses of more than \$50,000 to over \$5 million.

FIGURE 3
Costs of losing critical applications and/or data



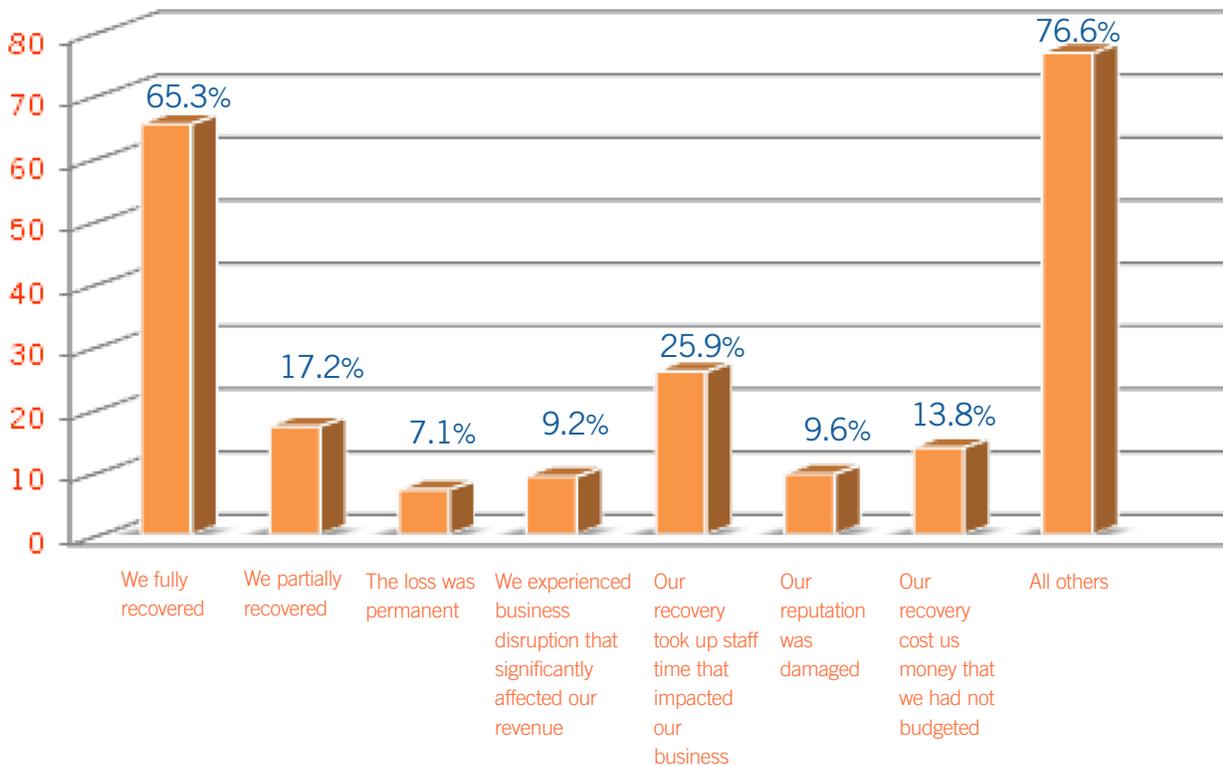
36.7%	No cost
18.3%	\$1000 - \$6000
12.5%	\$6001 - \$10,000
7.5%	\$10,001 - \$20,000
5.4%	\$20,001 - \$50,000
10%	\$50,001 - \$100,000
3.3%	\$100,001 - \$500,000
2.5%	\$500,001 - \$1 Million
1.7%	\$1 Million - \$5 Million
2.1%	Over \$5 Million



Business disruption adds to damage

In addition to direct dollar cost losses from outages and disasters, respondents experienced serious business disruption. While most organizations reported they were able to fully recover data, nearly one in five could only partially recover data and 7% of respondents indicated a permanent loss of data. More than a quarter of respondents indicated outages cost them valuable staff time, while one in ten indicated damage to their business reputation from an outage.

FIGURE 4
Resulting business disruption from outages/disasters





Outage/Data Loss Causes

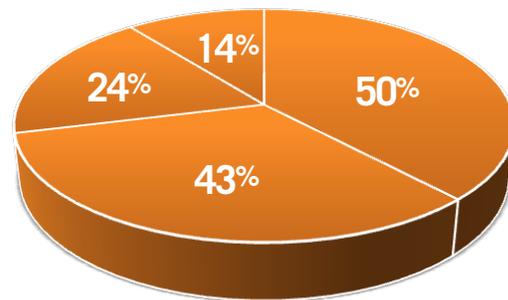
For most organizations, the question is not if a disaster or outage could happen, but when it will occur and how severe it will be. Most important, they need to ask themselves how prepared they will be to recover from a disaster scenario.

When evaluating the causes of outages, survey respondents indicated technology failures and human error as the major culprits. For the majority of organizations, software and hardware failures were the biggest cause of outages and data loss, while human error ran a close second at more than 40%.

Note the high percentage of human error contributing to outage or disaster. Too many organizations only check backups in severe weather when more realistically, the outage can happen at any time due to human error. Disaster preparedness has to be an ongoing activity.

FIGURE 5
Major causes of outages and data loss

- 50% software failure + network failure
- 43.5% human error
- 24% power failure
- 14% weather



Beyond the obvious causes of outages and disaster scenarios, the survey suggests that several factors influence the lack of preparedness among organizations worldwide.



Lack of Comprehensive DR Planning

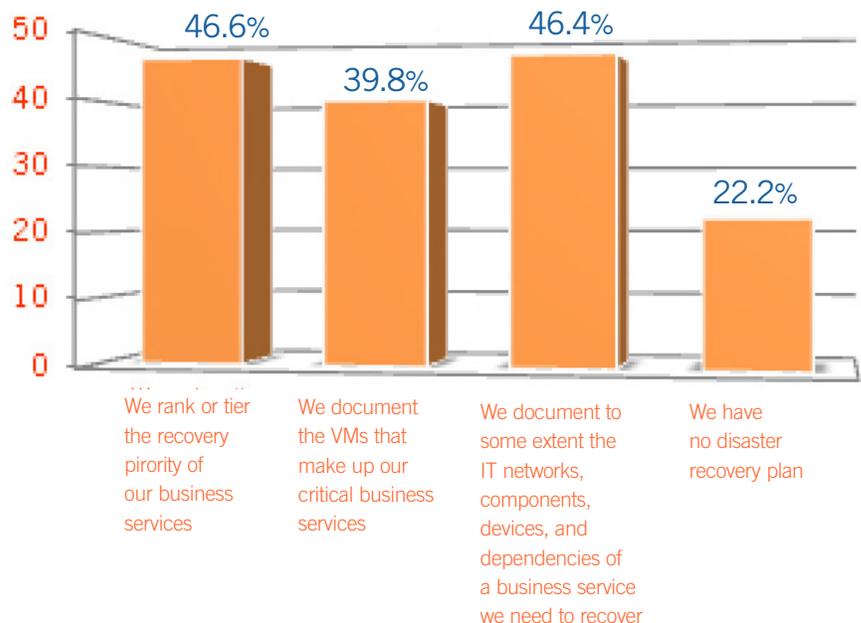
DR planning is clearly a sore spot for organizations seeking to protect their organizations from outages and data loss. More than 60% of those who took the survey do not have a fully documented DR plan and another 40% admitted that the DR plan they current have did not prove very useful when it was called on to respond to their worst disaster recovery event or scenario. Currently, DR planning has been and remains an imperfect science for most organizations, often posing as much uncertainty and risk as it is intended to alleviate.

FIGURE 6
Disaster Recovery planning falls short

	FULLY	SOMEWHAT	NOT DOCUMENTED	NOT APPLICABLE
Our disaster recovery plan is documented	30.89%	39.6%	14.2%	15.4%
Our disaster recovery plan identifies critical applications we need to recover and the components that make up these criitcal applications	32.1%	37.5%	12.9%	17.5%
Our disaster recovery plan documents Recovery Time Objects	31.3%	27.1%	23.8%	17.9%
Our disater recovery plan documents Recovery Point Objects	28.3%	31.7%	23.3%	16.7%
Our disaster recovery plan documents failover/failback processes	27.8%	33.2%	22.0%	17.0%

54% of those who took the survey do not have a fully documented DR plan

33% said their DR plan did not prove very useful in their worst DR event, while another third had no DR plan at all for their worst outage

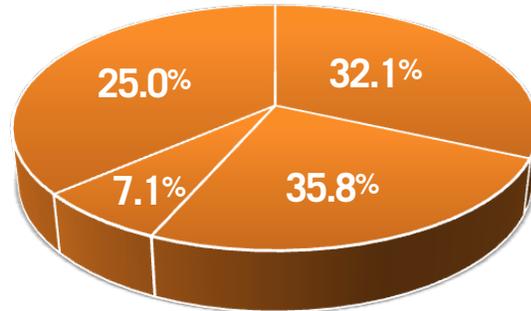




Perhaps even more alarming than the lack of planning for disaster recovery, it appears that DR test plans did not exist or were not very useful in the worst outage or data loss event experienced by two-thirds of survey respondents.

FIGURE 7

- 35.8% Did not have a DR test for this event
- 32.1% Very useful
- 25.0% Somewhat useful
- 7.1% Not useful

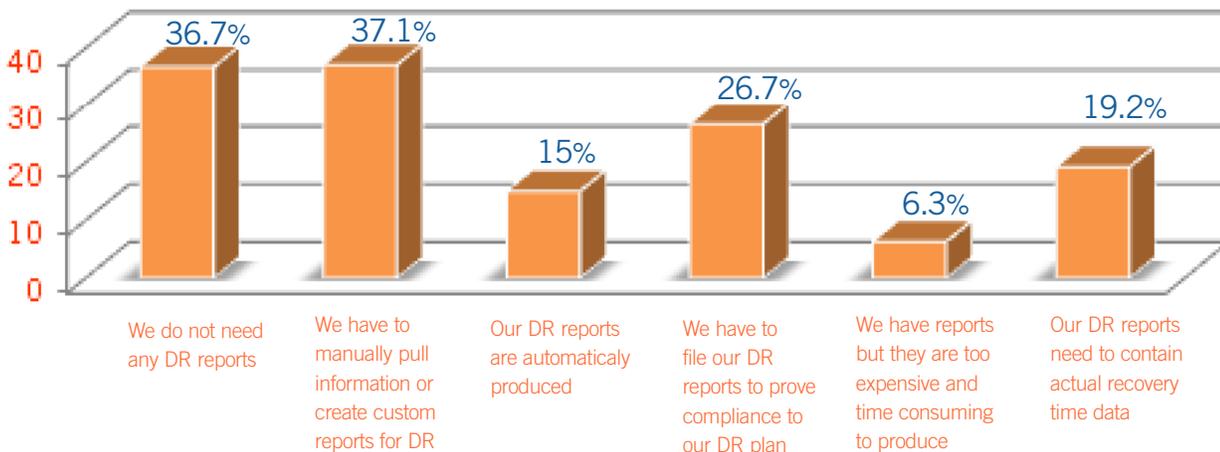


While the vast majority of organizations are required by regulations or policies to produce reports on DR preparedness, most organizations face an ongoing struggle with DR compliance reporting. The survey shows that 65% of companies need to produce DR reports for things such as compliance, while 43% find compliance reporting overly difficult, manual and expensive. In fact, only 15% of organizations can automatically produce reports on their DR activities. These results suggest that compliance reporting for DR is an area ripe for automation and innovation.

FIGURE 8

DR reporting is a struggle with manual methods

- 65% required to produce DR reports
- 43% find compliance reporting overly difficult, manual and expensive
- Only 15% have the ability to automatically produce DR reports



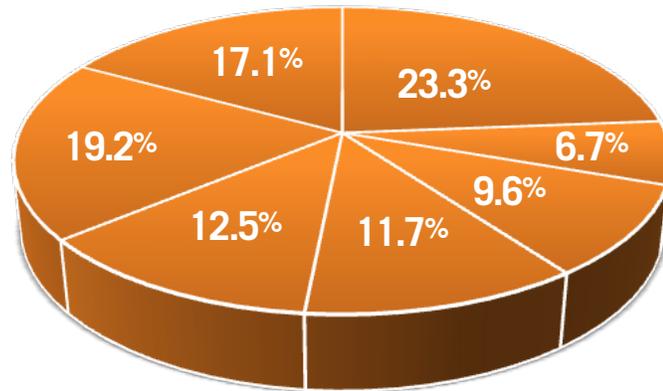


Lack of DR Testing

Unfortunately, a third of all organizations participating in the survey test their DR plans only once or twice a year and fully 23% or one in four never test their DR plans. Without testing and verification of DR plans, most companies really have no idea as to whether they can fully recover their IT systems in the event of a disaster or extended outage.

FIGURE 9
DR testing rare for most organizations

6.7%	Weekly
9.6%	Monthly
11.7%	Quarterly
12.5%	Twice a year
19.2%	Annually
17.1%	At unspecified intervals
23.3%	Never



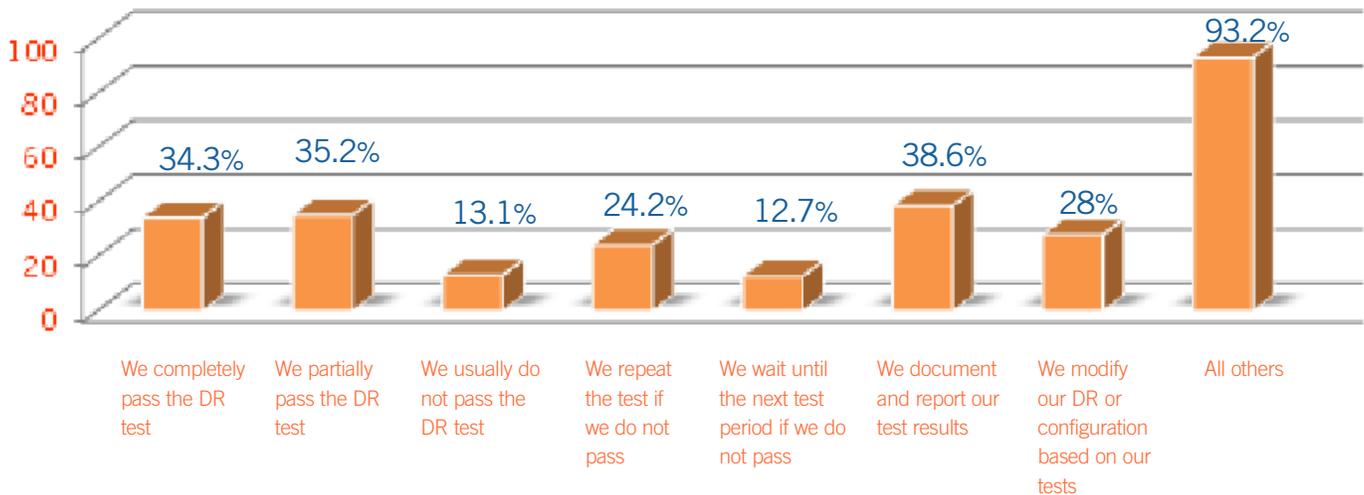
When companies do test their DR plans, the results are most disturbing. More than 65% do not pass their own tests! But the challenges of DR testing go even deeper for many organizations. More than half of those who actually test DR plans don't document the results of their tests.

Even among those organizations that test more often, including weekly or monthly, nearly two-thirds have inadequate or undocumented RTO/RPO/failover, failback processes with fully one out of four having no test documentation at all. Without documenting/measuring Recovery Time Actuals (RTA's) against Recovery Time Objectives and Recovery Point Objectives, there is simply no way of judging how well failover/failback processes might function in the event of an outage or disaster.

Most alarming of all, only one in four of those organizations who fail the first round of DR testing, ever actually re-test as part of their follow up.



FIGURE 10
DR testing failing by every measure



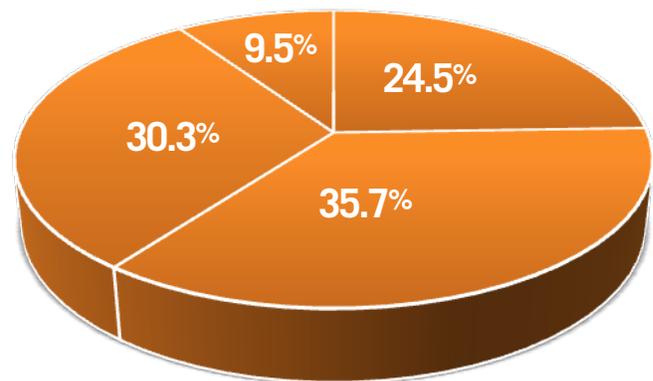
The results of the survey related to DR testing are of particular concern to the DR Preparedness Council. They point to the need for a major shift in the way DR testing is conducted so that organizations can automate the testing of critical IT components and applications and thus allow testing to be much more frequent and affordable.

Lack of DR Resources in terms of Budget and Skills

Nearly two-thirds of respondents believe that DR is underfunded, with nearly half unsure about what is spent for DR or having no budget allocation at all.

FIGURE 11
DR budgets inadequate and underfunded for most organizations

- 35.7% Funded adequately
- 30.3% Somewhat underfunded
- 9.5% Significantly underfunded
- 24.5% No funding

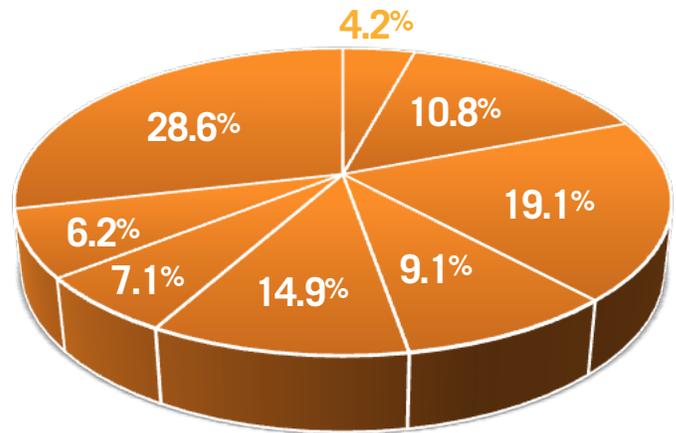




Most of the respondents to the survey possess secondary sites that help to serve as repositories for backup data and therefore do not measure spending on DR as a separate budget item per se. The industry average among those who do measure DR spending indicated between 2% and 7% of their IT budget is devoted to DR activities.

FIGURE 12
Percent of total IT budget allocated to DR activities

4.2%	Each business unit handles its own DR budget
0%	14.9%
1-4%	19.1%
5-7%	9.1%
8-10%	10.8%
11-15%	6.2%
over 15%	7.1%
We do not measure	28.6%



Many organizations today still struggle with assembling the skills, time or money to adequately plan and test their DR preparedness.

- 21% do not have the skill sets to effectively perform DR tests
- 36% do not have the time to test their DR plans
- 18% say DR is too expensive to test
- 26% say that each DR test costs between \$5,000 - \$50,000

For organizations worldwide to improve their DR preparedness, we as an industry must seek out and develop better tools and solutions to automate processes and overcome the high cost in time and money of verifying and testing DR plans.



Part 2

Best Practices from Better Prepared Organizations

While survey respondents scoring top grades on the benchmark survey are a smaller percentage than those struggling with DR preparedness, the results of the survey suggest several practices that distinguish those organizations more prepared compared to their colleagues. The apparent best practices fall into four broad categories:

More prepared organizations implement more detailed DR plans

Results from the survey indicate that those organizations scoring in the top tiers (A's and B's) fit a specific DR Plan profile with particular characteristics. The hallmarks of a good DR plan are much more than lists of emergency phone numbers built into call trees.

Top scoring organizations, for example, have a much higher percentage of fully documenting their disaster recovery plans. In contrast, nearly one third of organizations with a failing grade have no DR plan at all.

At the same time nearly all top tier scoring participants clearly identify critical applications and their vital components that they need for recovery. In contrast, only one in five organizations scoring in the lower tiers (D's and F's) fully document their DR plans or identify critical applications to be recovered.

In addition, the vast majority of top tier scoring organizations detail failover/failback processes in their DR documentation.

More prepared organizations set specific DR metrics for RTOs and RPOs

Organizations that define specific Recovery Time Objectives and Recovery Point Objectives for each of their mission critical business services such as Customer Orders, Finance, and Email, exhibited much higher benchmark scores. Building a DR plan with detailed objectives and then following through by testing those objectives with planned failures enables an organization to practice their Disaster Recovery Plan and make refinements to improve it. These organizations not only scored well but they achieve true confidence in their DR preparedness.

In addition, persistence in DR Planning, as in most other practices, pays off: organizations that make adjustments and repeat DR tests that fail, as well as updating their DR plans as their configurations change, were among the top scorers.



More prepared organizations test DR plans much more frequently

Transparency also played a major role in high-scoring DR plans. Companies that publish their DR results were most often in the higher scoring categories and those that had a compliance regulation to publish them were even higher. Thus, testing a DR plan as often as possible results in a much better, more actionable and reliable DR Plan. Interestingly, allocating specific funds for DR did not appear to significantly influence high scores.

Many organizations indicated they had no DR budget or had an underfunded DR budget

However, their DR plans could still be detailed and kept up-to-date as a company discipline rather than specifically designated as an expense item in their IT budgets.

Spending a lot of money on DR tests was not necessarily a strong indicator of a good DR plan. Most organizations spent well under \$50,000 on DR testing. In fact, 23% of respondents kept their DR testing under \$5,000 annually. This encouraging statistic suggests that testing DR can be relatively inexpensive if the virtualization infrastructure is in place to support it. Given that most benchmark participants had a secondary data center with hardware or software replication or mirroring indicates that many organizations have standby failover policies in place, helping to reduce the cost of testing.

Finally, a good DR plan must be actively tested and implemented. High scoring organizations were implementing DR, planning DR, or revising/migrating their DR plan. Organizations that merely write a plan and file it away are simply not as secure in their recovery as those that regularly test, update, and document their DR plans.

Part 3

What You Can Do to Increase Your DR Preparedness

The question is not if a disaster or outage could happen, but when it will occur and how prepared your organization will be for that scenario. That's why the DR Preparedness Council members recommend that 2014 be the year that your organization gets serious about planning and testing disaster recovery with these three steps:

Build a DR plan for everything you need to recover

There are many items that IT professionals must recover. Companies need to protect their data, files, folders, emails, etc. They also need to recover applications, networks and document repositories, business services such as the entire order processing system, or even their entire site in the event of an outage or disaster.



Define Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO) for critical applications

RTOs are all about defining how quickly you need to recover. This describes the amount of downtime that is tolerable in the event of an outage or disaster. RPOs describe the amount of data you are willing to risk in an outage or disaster. Companies need to define RTOs and RPOs for critical applications. Without these important metrics, you cannot set proper expectations and assumptions from management, employees, and customers about your DR capabilities and how to improve them.

Test critical applications frequently to validate they will recover within RTOs/RPOs

Companies need to position themselves to immediately become aware when the recovery time or recovery point actuals do not fall within their objectives. For DR preparedness to improve, companies must automate these processes to overcome the high cost in time and money of verifying and testing their DR plans.

By implementing these three steps, you will have made a significant contribution to ensuring business continuity regardless of industry or evolving threats.

Start by taking the Benchmark Survey for yourself

Participants who complete the survey, receive a grade (A-F) indicating the level of disaster recovery preparedness their organization has reached. They then receive an email with a report that shows how individual responses compare to those of all other survey participants. Personal and identifying information about each organization is strictly confidential and will not be revealed to other survey participants or the public in any way. All responses are anonymous but available to each participant as totals that allow you to make your own comparisons. The survey takes about 10 minutes to complete and nearly every question requires an answer so that the resulting benchmark database will be consistent.



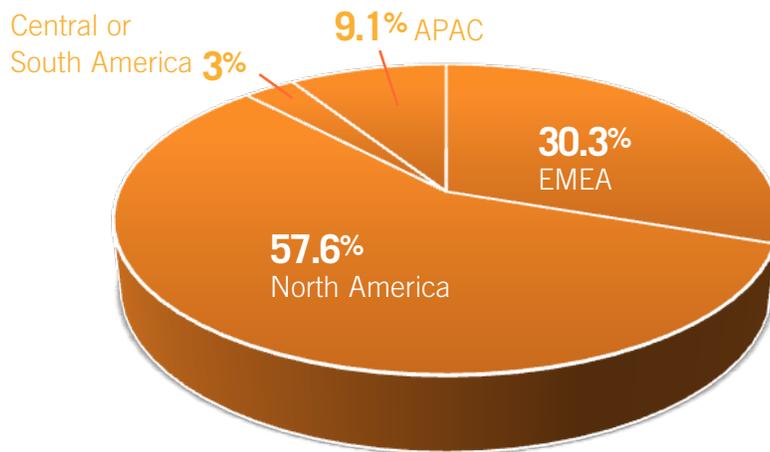
About the survey

The DRPB survey provides a benchmarking score from 0-149 that measures the implementation of IT DR best practices. DRPB benchmarking scores parallel the grading system familiar to most students in North America whereby a score over 119 is an A or superior grade; 103 to 118 is a B or above average grade; 70-79 87 to 102 is a C or average grade and 71-86 is a D or unsatisfactory grade. Below 70, rates as an F, or failing grade.

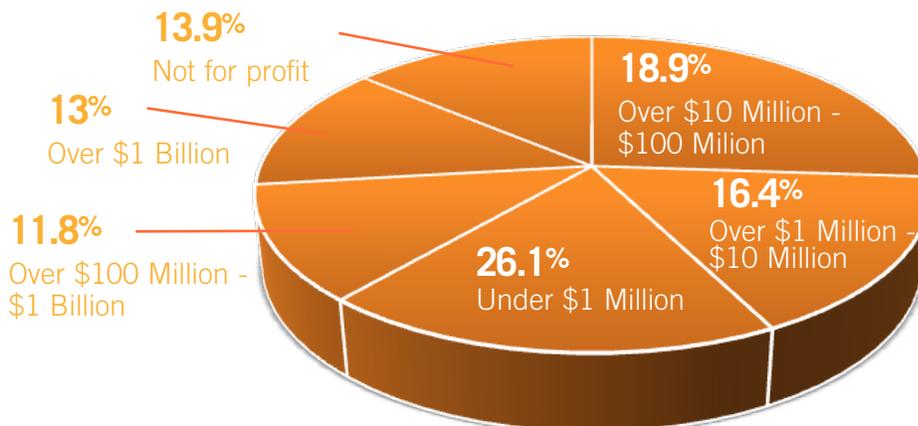
The 243 participants of the survey used in this Annual Report represent a broad cross section of organizations throughout the world. Key characteristics among participants include:

Geographic location

This benchmark survey represents one of the most comprehensive global studies of DR Preparedness that we are aware of, representing a broad range of industries, company sizes & responses from IT professionals managing business continuity and disaster recovery every day.



Size of participant organization revenues





Role within the organization

More than one in ten survey respondents have an official title/role designated for business continuity and disaster recovery, while most share responsibility for DR among other roles and responsibilities.

2.5%	Compliance Officer or Auditor
4.2%	Line of Business or Department Manager
????	Business Continuity or Disaster Recovery Office
7.1%	Non-IT Executive Management
10.9%	IT/IS Staff
12.6%	Executive IT Management
21.8%	IT Director/Manager
33.9%	All others

Disaster recovery is a requirement for many

For nearly half of the survey participants, disaster recovery is a requirement either through legal regulations or company policy.

49.8%	Yes
36.4%	No
13.8%	I'm not sure

Percentage of virtualized servers

Nearly one third of survey participants have 75% or more of their IT environments virtualized.

31.5%	Over 76%
29.4%	Less than 10%
15.1%	51-75%
14.3%	26-50%
9.7%	11-25%



About the DR Preparedness Council

As recent cyber-attacks and natural disaster events such as Hurricane Sandy have shown, the need for IT disaster recovery preparedness has never been greater. Yet research shows that less than half of all companies using IT have a disaster recovery plan in place, and even fewer have actually tested their plans to see if they will work as expected. Clearly there is a need to appreciate the value of disaster recovery planning and testing as well as gain a better understanding of DR best practices to make preparedness more cost-effective and efficient.

The IT Disaster Recovery Preparedness (DRP) Council has been formed by IT business, government and academic leaders to address these issues. Our mission is to increase DR Preparedness awareness, and improve DR practices. To help achieve that goal the Council has developed an online IT Disaster Recovery Preparedness Benchmark survey. The survey is designed to give business continuity, disaster recovery, compliance audit and risk management professionals a measure of their own preparedness in recovering critical IT systems running in virtual environments.

For more information about the Disaster Recovery Preparedness Council visit our website at www.drbenchmark.org, or contact us at info@drbenchmark.org