



Your Benchmark Comparison Report

Survey: IT Disaster Recovery Benchmark

Welcome to the Disaster Recovery Benchmark Survey from the IT Disaster Recovery Preparedness Council. This benchmark has been created by the IT Disaster Recovery Preparedness Council to collect metrics and comparisons on behalf of the Disaster Recovery industry. This IT Disaster Recovery Benchmark allows your organization to participate in a global survey on DR best practices as well as gauge how your results compare to your peer group.

Once you have completed the survey, you will receive a grade (A-F) indicating the level of disaster recovery preparedness your organization has reached. Then, as a benchmark participant, you will receive an email with a report that shows how your responses compare to those of the other participants. Make sure you enter the email address you want to use to receive your report in the survey below.

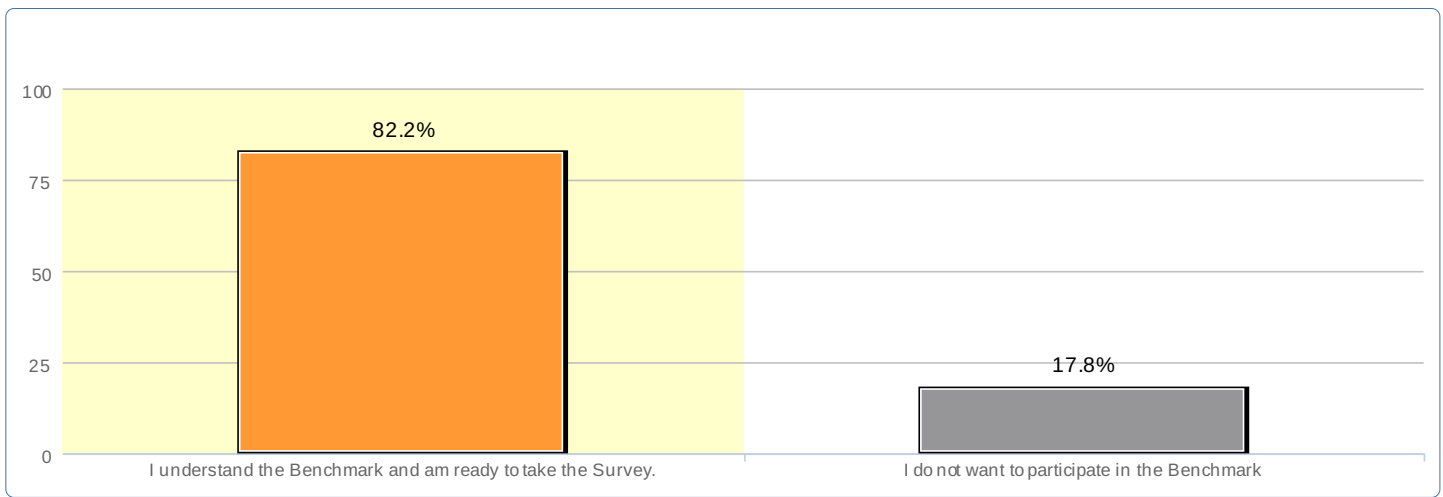
Personal and identifying information about you and your organization are strictly confidential and will not be revealed to other survey participants or the public in any way. All responses are anonymous but available to you as totals to allow you to make your own comparisons.

This survey will take approximately 10 minutes to complete and nearly every question requires an answer so that the resulting benchmark database will be consistent.

This 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.

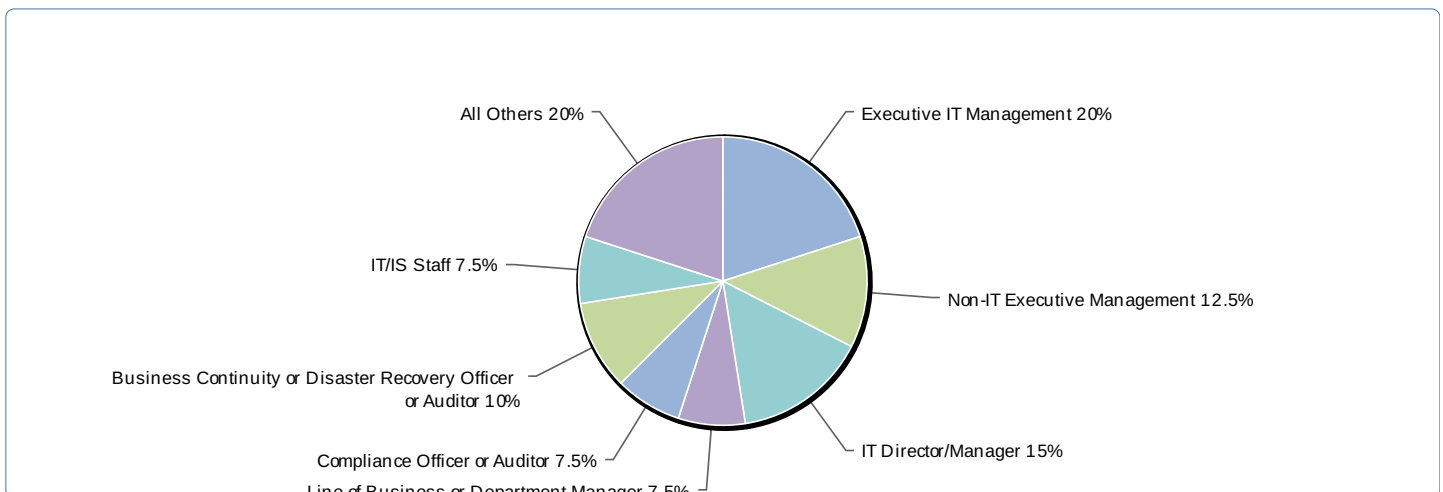
Use the following checklist to ensure your organization can benefit from this benchmark. You must check at least one of the options below to qualify to take the survey. My company/organization meets the following conditions:

Value	Percent %
I understand the Benchmark and am ready to take the Survey.	82.2%
I do not want to participate in the Benchmark	17.8%



What is your role at your organization?

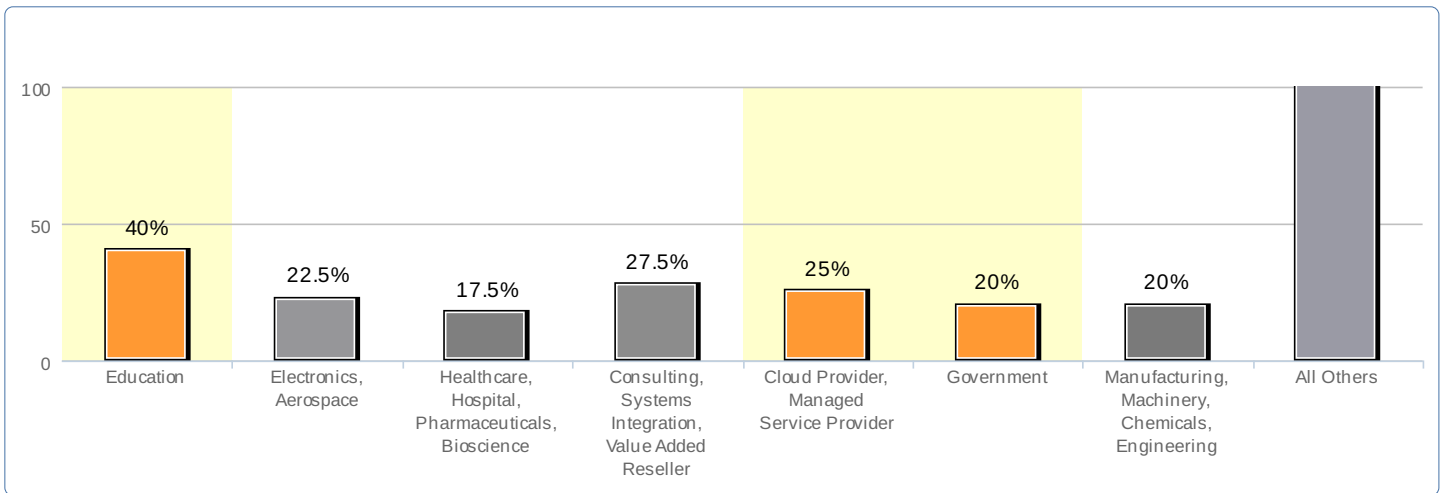
Value	Percent %
Executive IT Management	20.0%
Non-IT Executive Management	12.5%
IT Director/Manager	15.0%
Line of Business or Department Manager	7.5%
Compliance Officer or Auditor	7.5%
Business Continuity or Disaster Recovery Officer or Auditor	10.0%
IT/IS Staff	7.5%
VAR/Systems Integrator	5.0%
Solutions Architect or Engineer	0.0%
Other Employee	5.0%
Other Consultant	10.0%



What Industry is your organization in?

Value	Percent %
Education	40.0%
Electronics, Aerospace	22.5%
Healthcare, Hospital, Pharmaceuticals, Bioscience	17.5%
Consulting, Systems Integration, Value Added Reseller	27.5%

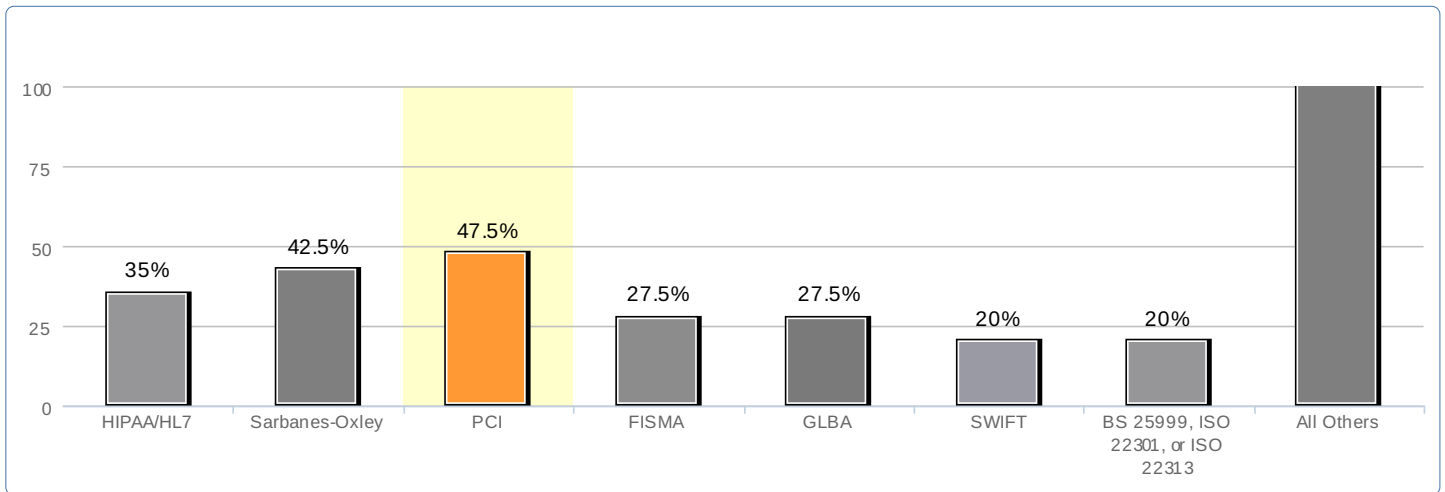
Cloud Provider, Managed Service Provider	25.0%
Government	20.0%
Manufacturing, Machinery, Chemicals, Engineering	20.0%
Energy, Utilities	17.5%
Construction, Real Estate	12.5%
Retail, Apparel	15.0%
Banking, Finance, Insurance, Legal	17.5%
Not for Profit	10.0%
Technology, Software	37.5%
Entertainment, Hospitality, Recreation, Sports	12.5%
Food, Agriculture	25.0%
Telecommunications	25.0%
Communications, Marketing, Journalism	22.5%
Transportation, Shipping	22.5%



Does your organization need to comply with any regulations? Check all that apply.

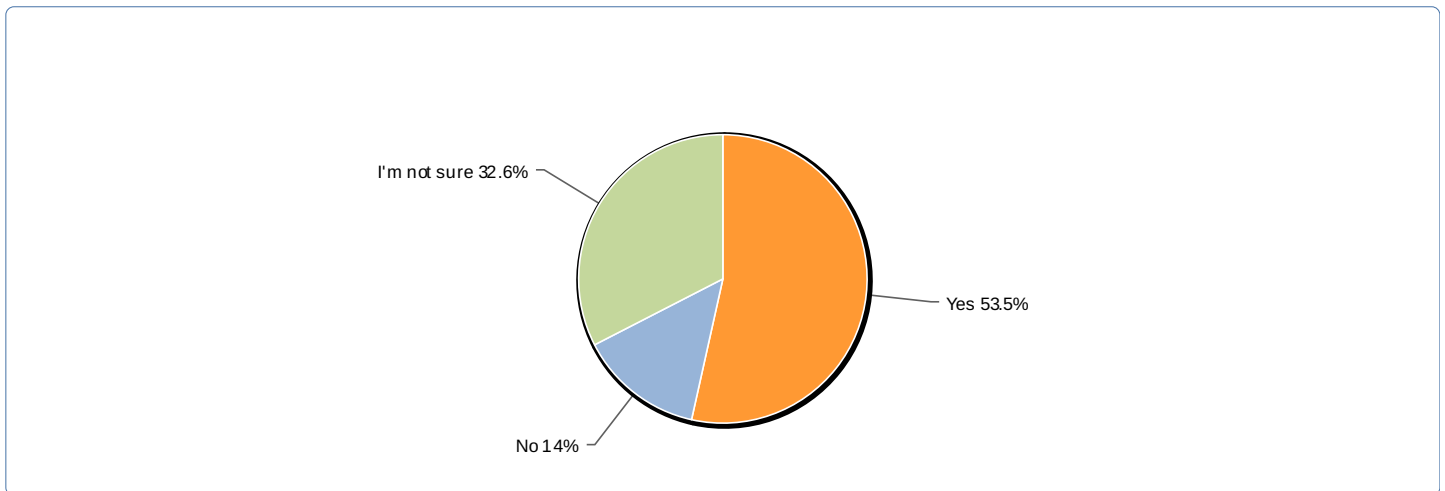
Value	Percent %
HIPAA/HL7	35.0%
Sarbanes-Oxley	42.5%
PCI	47.5%
FISMA	27.5%
GLBA	27.5%
SWIFT	20.0%
BS 25999, ISO 22301, or ISO 22313	20.0%
COBIT	47.5%
NIST	22.5%
BASEL II	22.5%
FERPA	27.5%
ISAAC	20.0%
None	45.0%
Other (please specify other regulation)	22.5%
IRS	0.0%

Statistics	
Sum	7.0
Avg.	2.3
StdDev	3.3
Max	7.0



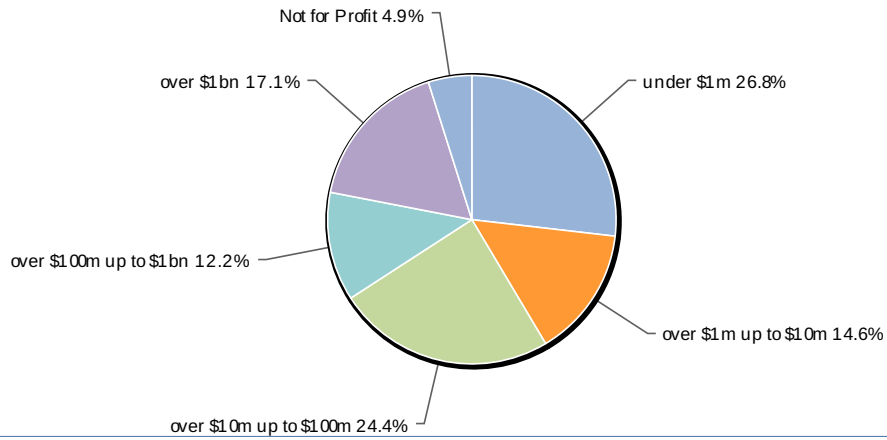
Is business continuity or disaster recovery a compliance requirement for your organization?

Value	Percent %
Yes	53.5%
No	14.0%
I'm not sure	32.6%



What is the annual revenue of your company/organization?

Value	Percent %
under \$1m	26.8%
over \$1m up to \$10m	14.6%
over \$10m up to \$100m	24.4%
over \$100m up to \$1bn	12.2%
over \$1bn	17.1%
Not for Profit	4.9%

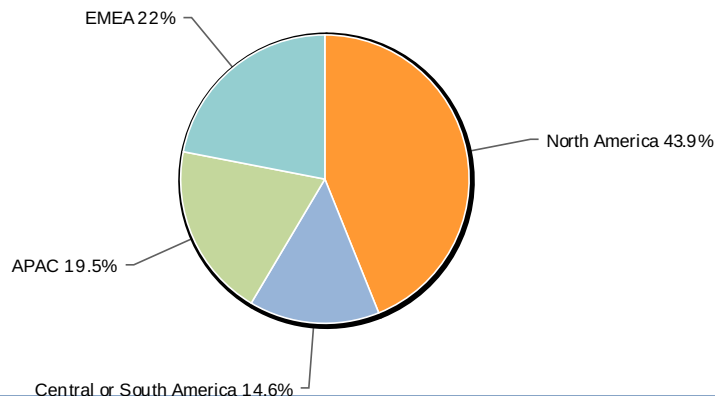


What is the approximate number of employees of your company/organization?

Value	Percent %
1 to 100 employees	0.0%
101 to 500 employees	0.0%
501 to 1000 employees	0.0%
1001 to 5000 employees	0.0%
5001 to 15000 employees	0.0%
over 15000 employees	0.0%

In which region is the headquarters of your company/organization?

Value	Percent %
North America	43.9%
Central or South America	14.6%
APAC	19.5%
EMEA	22.0%

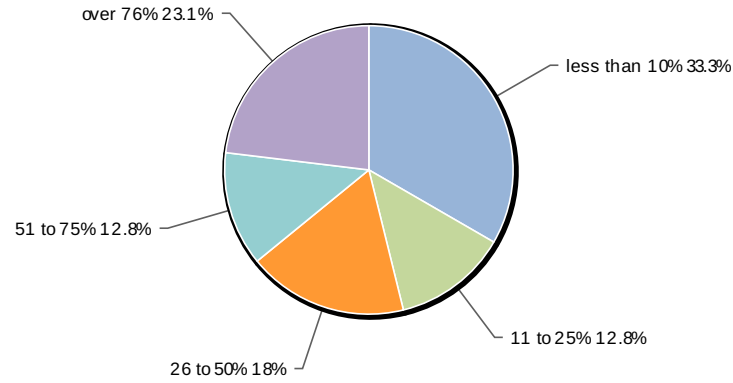


What % of your servers are virtual?

Value	Percent %	Statistics	
less than 10%	33.3%	Sum	492.0

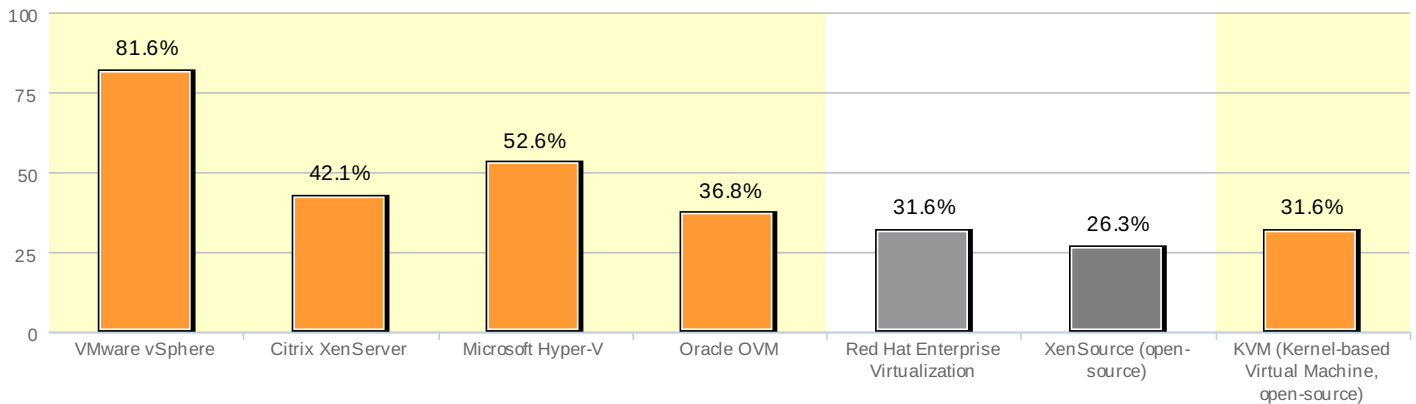
11 to 25%	12.8%
26 to 50%	18.0%
51 to 75%	12.8%
over 76%	23.1%

Avg.	28.9
StdDev	15.5
Max	51.0



Please tell us about your hypervisor environment. Check all that apply if you have deployed the hypervisor or are planning to deploy it

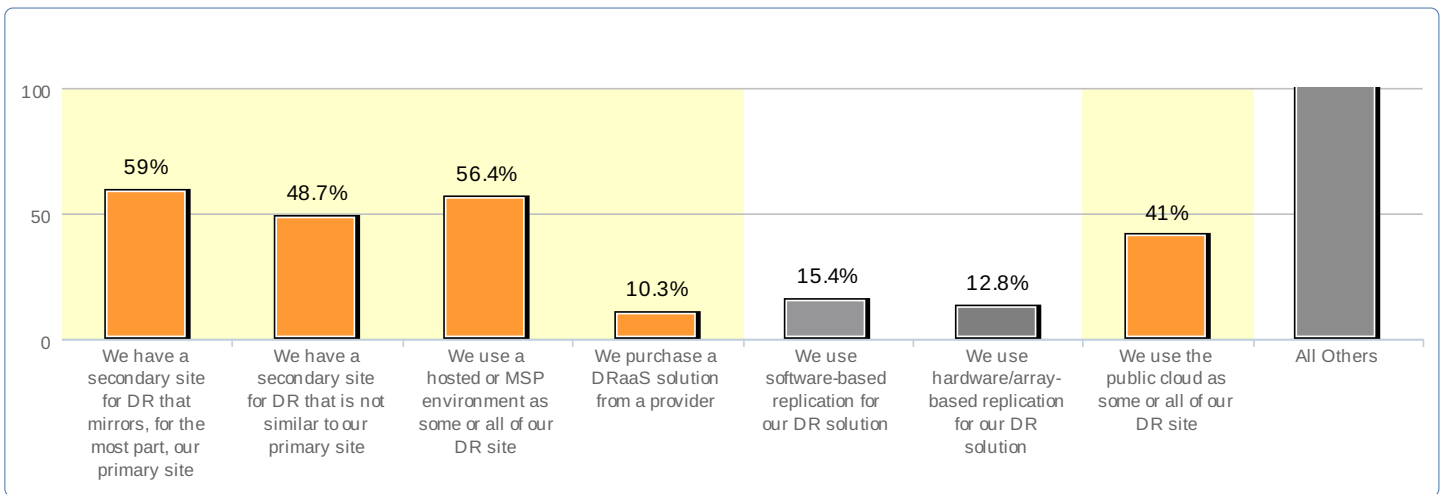
Value	Percent %
VMware vSphere	81.6%
Citrix XenServer	42.1%
Microsoft Hyper-V	52.6%
Oracle OVM	36.8%
Red Hat Enterprise Virtualization	31.6%
XenSource (open-source)	26.3%
KVM (Kernel-based Virtual Machine, open-source)	31.6%



Please describe your disaster recovery implementation. Check all that apply.

Value	Percent %
We have a secondary site for DR that mirrors, for the most part, our primary site	59.0%

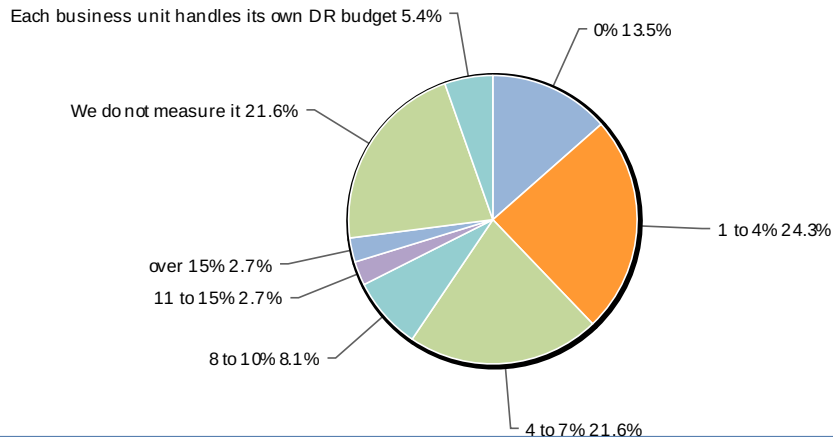
We have a secondary site for DR that is not similar to our primary site	48.7%
We use a hosted or MSP environment as some or all of our DR site	56.4%
We purchase a DRaaS solution from a provider	10.3%
We use software-based replication for our DR solution	15.4%
We use hardware/array-based replication for our DR solution	12.8%
We use the public cloud as some or all of our DR site	41.0%
We use additional machines and devices in our primary site for our disaster recovery	46.2%
We use high availability hardware or software as part of our DR plan	46.2%
We use data or application mirroring for DR	51.3%
We are implementing our DR plan currently	38.5%
Our DR implementation is being revised/migrated	46.2%
Our DR implementation is completed other than planned upgrades and maintenance	35.9%
Our DR implementation is in the planning stage	43.6%



What percentage of your IT budget is allocated to IT Disaster Recovery this year?

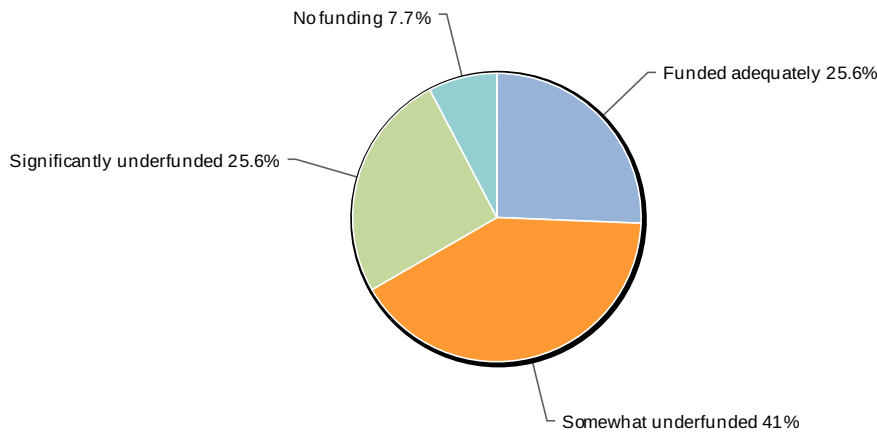
Value	Percent %
0%	13.5%
1 to 4%	24.3%
4 to 7%	21.6%
8 to 10%	8.1%
11 to 15%	2.7%
over 15%	2.7%
We do not measure it	21.6%
Each business unit handles its own DR budget	5.4%

Statistics	
Sum	76.0
Avg.	3.6
StdDev	2.9
Max	11.0



Is your IT Disaster Recovery budget funded adequately?

Value	Percent %
Funded adequately	25.6%
Somewhat underfunded	41.0%
Significantly underfunded	25.6%
No funding	7.7%

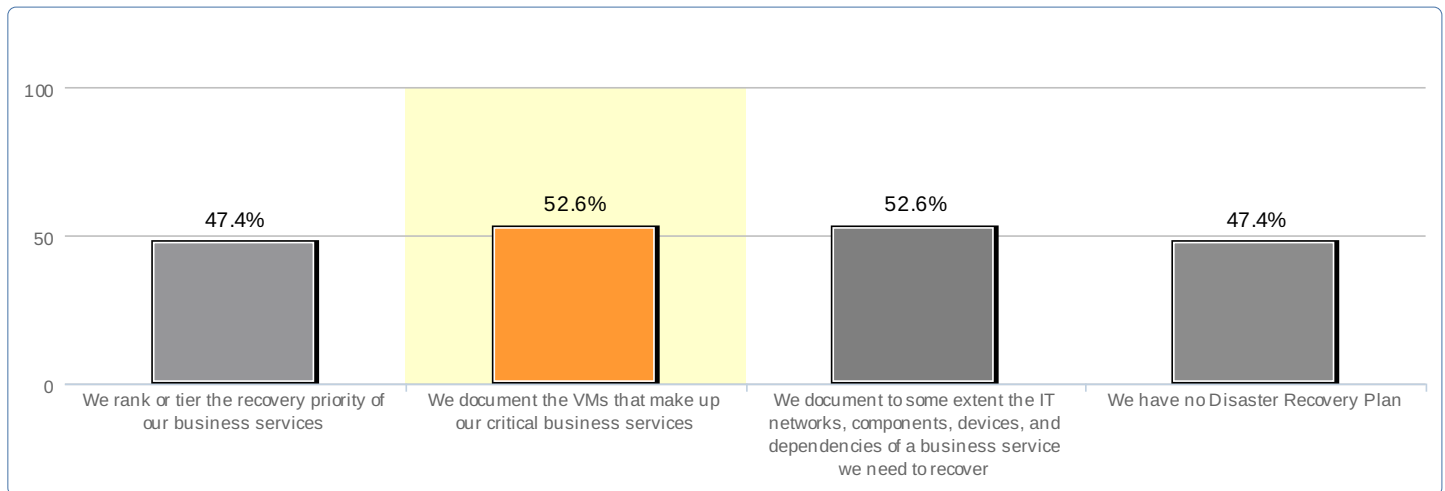


Does your company/organization have a documented IT Disaster Recovery Plan? You are half way done with the survey! Please continue to ensure your answers are consistent and represent your actual DR status.

	Fully	Somewhat	Not Documented	Not applicable	Avg.
Our Disaster Recovery Plan is documented	26.7%	33.3%	26.7%	13.3%	0.0
Our Disaster Recovery Plan identifies critical applications we need to recovery and the components that make up these critical applications	26.7%	42.2%	15.6%	15.6%	0.0
Our Disaster Recovery Plan documents Recovery Time Objectives	20.0%	37.8%	33.3%	8.9%	0.0
Our Disaster Recovery Plan documents Recovery Point Objectives	28.9%	33.3%	24.4%	13.3%	0.0
Our Disaster Recovery Plan documents failover/failback processes	26.7%	26.7%	24.4%	22.2%	0.0
Average %	25.8%	34.7%	24.9%	14.7%	0.0

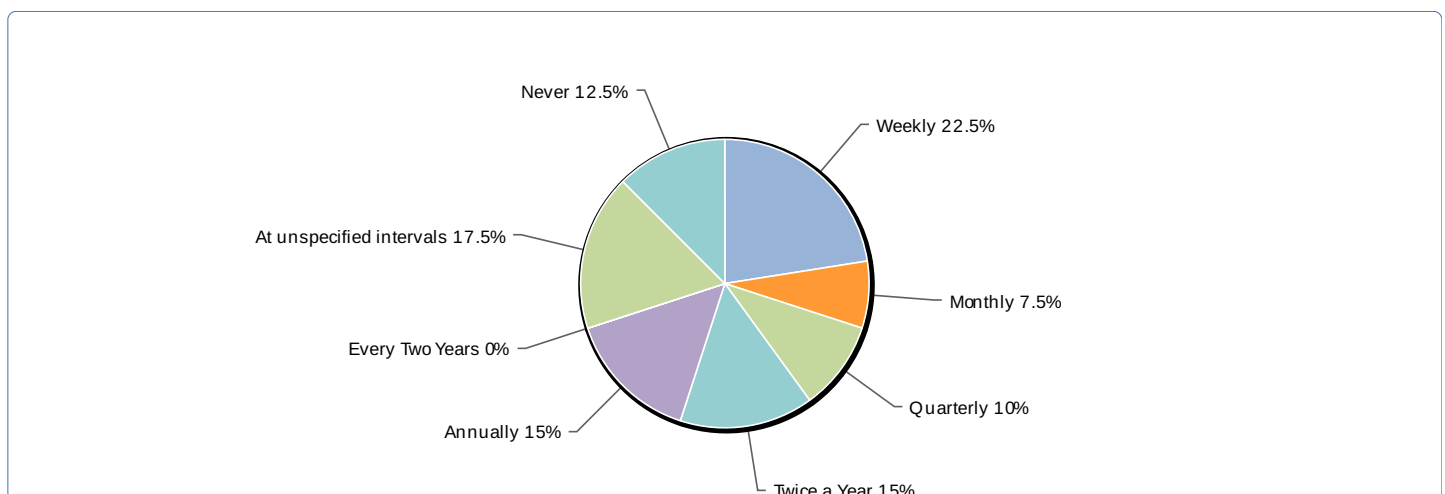
Our company/organization has identified our critical business services to recover in the event of a disaster. Check all that apply.

Value	Percent %
We rank or tier the recovery priority of our business services	47.4%
We document the VMs that make up our critical business services	52.6%
We document to some extent the IT networks, components, devices, and dependencies of a business service we need to recover	52.6%
We have no Disaster Recovery Plan	47.4%



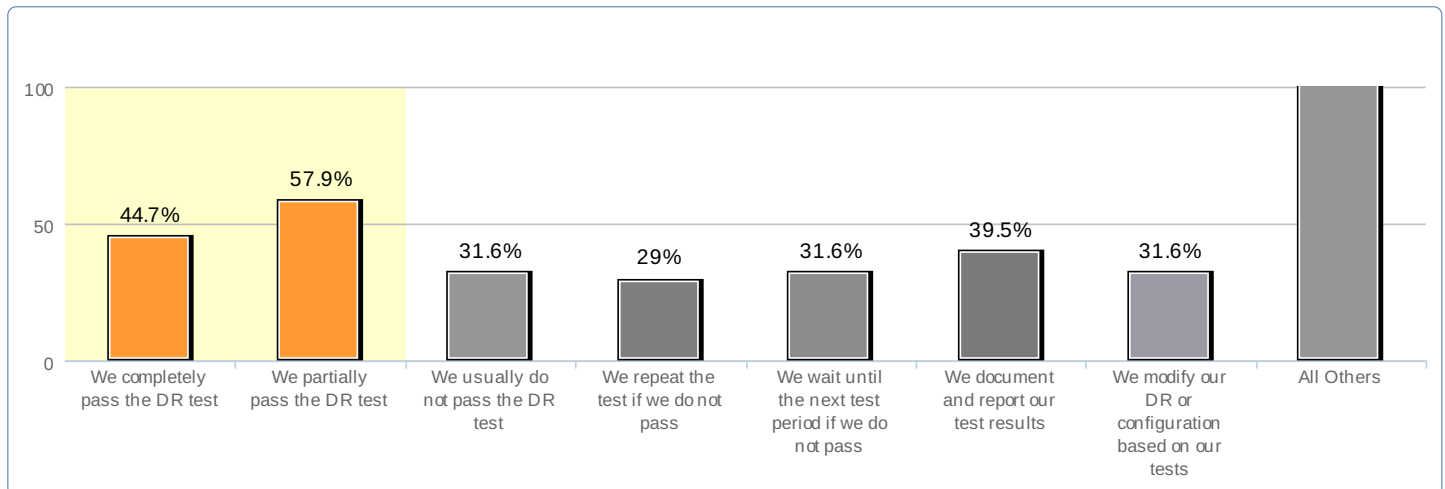
My company/organization tests our Disaster Recovery Plan

Value	Percent %
Weekly	22.5%
Monthly	7.5%
Quarterly	10.0%
Twice a Year	15.0%
Annually	15.0%
Every Two Years	0.0%
At unspecified intervals	17.5%
Never	12.5%



When we test our disaster recovery plan, we have the following results. Check all that apply.

Value	Percent %
We completely pass the DR test	44.7%
We partially pass the DR test	57.9%
We usually do not pass the DR test	31.6%
We repeat the test if we do not pass	29.0%
We wait until the next test period if we do not pass	31.6%
We document and report our test results	39.5%
We modify our DR or configuration based on our tests	31.6%
We have a compliance need to test our DR plan	23.7%
We have a company/organization need to test our DR plan	34.2%
We have a company/organization policy or SLA to test our DR plan	42.1%
We test our Recovery Time Objectives and/or Recovery Point Objectives	34.2%
Testing DR is part of a hosted, MSP, or CSP service we engage in	36.8%



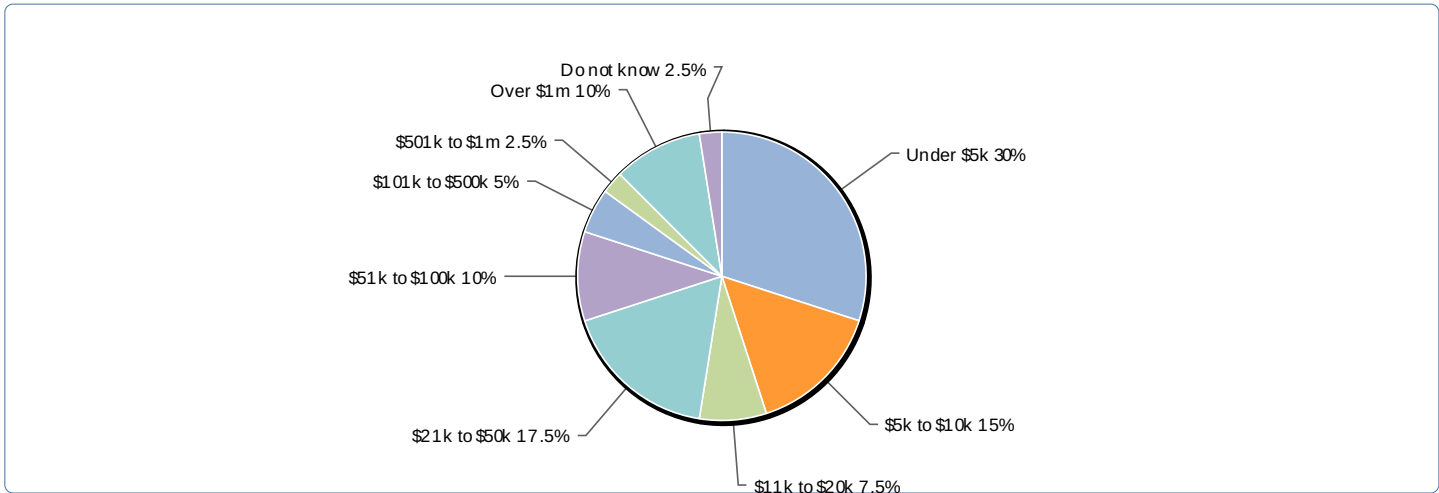
We have encountered the following in testing out DR plan.

	Hardly Ever	Seldom	Often	Nearly Every Time	Not Applicable	Avg.
Configuration changes cause our DR test to fail or halt	20.0%	26.7%	22.2%	11.1%	20.0%	0.0
Our DR plan is too expensive to test	24.4%	22.2%	15.6%	22.2%	15.6%	0.0
Resources have time to test our DR plan	40.0%	24.4%	20.0%	6.7%	8.9%	0.0
Resources have skill to test our DR plan	28.9%	26.7%	15.6%	13.3%	15.6%	0.0
Our DR plan helps us create good tests	33.3%	33.3%	13.3%	8.9%	11.1%	0.0
Average %	29.3%	26.7%	17.3%	12.4%	14.2%	0.0

What do your DR tests cost your organization annually (include time, resources, equipment)?

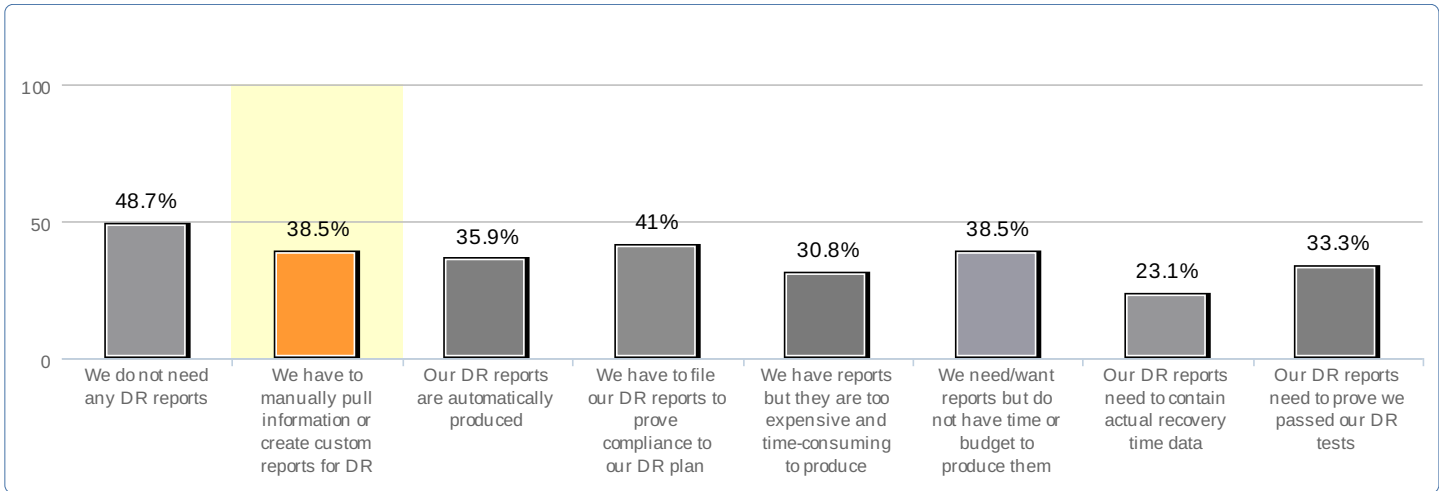
Value	Percent %
Under \$5k	30.0%
\$5k to \$10k	15.0%
\$11k to \$20k	7.5%
\$21k to \$50k	17.5%
\$51k to \$100k	10.0%

\$101k to \$500k	5.0%
\$501k to \$1m	2.5%
Over \$1m	10.0%
Do not know	2.5%



Do you need to produce Disaster Recovery reports? If so, check all that apply.

Value	Percent %
We do not need any DR reports	48.7%
We have to manually pull information or create custom reports for DR	38.5%
Our DR reports are automatically produced	35.9%
We have to file our DR reports to prove compliance to our DR plan	41.0%
We have reports but they are too expensive and time-consuming to produce	30.8%
We need/want reports but do not have time or budget to produce them	38.5%
Our DR reports need to contain actual recovery time data	23.1%
Our DR reports need to prove we passed our DR tests	33.3%



We have a Disaster Recovery Management Team who will execute our Disaster Recovery Plan in the event of a disaster.

	Fully	Partly	Inadequately	Not at	Not	Avr
--	-------	--------	--------------	--------	-----	-----

	Fully	Partly inadequate	Partly adequate	Not applicable	Avg.	
Our Disaster Recovery Management Team is documented with upto date contacts	33.3%	22.2%	15.6%	17.8%	11.1%	0.0
Our Disaster Recovery Management Team has a documented contact or call tree with upto date information	24.4%	24.4%	24.4%	15.6%	11.1%	0.0
Our Disaster Recovery Management Team has a documented definition of their roles during a disaster	24.4%	28.9%	26.7%	13.3%	6.7%	0.0
Our Disaster Recovery Management Team has a documented definition of a "disaster"	22.2%	31.1%	11.1%	26.7%	8.9%	0.0
Our Disaster Recovery Management Team practices or trains on our DR plan.	17.8%	20.0%	31.1%	15.6%	15.6%	0.0
Our employees understand their role in the DR Plan	26.7%	24.4%	13.3%	8.9%	26.7%	0.0
Average %	24.8%	25.2%	20.4%	16.3%	13.3%	0.0

Only a few questions remain! The remainder of this benchmark survey gathers information about your disaster recovery experiences. This allows you to gauge your risk of a disaster by seeing what others have experienced. Please click the radio button that best describes the amount of down time you experienced for the type of data loss.

	For hours	For days	For weeks	Permanently	Never experienced this loss	Not applicable	Avg.
Lost one virtual machine	24.4%	24.4%	13.3%	13.3%	15.6%	8.9%	0.0
Lost one host machine	42.2%	17.8%	17.8%	4.4%	11.1%	6.7%	0.0
Lost one critical application	40.0%	13.3%	13.3%	6.7%	13.3%	13.3%	0.0
Lost multiple virtual machines	37.8%	15.6%	4.4%	8.9%	20.0%	13.3%	0.0
Lost multiple host machines	40.0%	15.6%	8.9%	6.7%	13.3%	15.6%	0.0
Lost multiple critical applications	37.8%	17.8%	4.4%	11.1%	15.6%	13.3%	0.0
Lost most or all of a data center	33.3%	13.3%	11.1%	8.9%	17.8%	15.6%	0.0
Lost less than half of storage	28.9%	15.6%	8.9%	17.8%	22.2%	6.7%	0.0
Lost more than half of storage	26.7%	8.9%	17.8%	15.6%	17.8%	13.3%	0.0
Lost network connectivity	40.0%	22.2%	0.0%	17.8%	13.3%	6.7%	0.0
Lost critical data/files	31.1%	15.6%	13.3%	11.1%	22.2%	6.7%	0.0
Backups/archives not recoverable	44.4%	13.3%	13.3%	8.9%	8.9%	11.1%	0.0
Replicas not recoverable	33.3%	15.6%	8.9%	13.3%	17.8%	11.1%	0.0
Archives not recoverable	20.0%	12.5%	7.5%	20.0%	25.0%	15.0%	0.0
Average %	34.4%	15.8%	10.2%	11.7%	16.6%	11.2%	0.0

Which of the following best describes where any of the losses below occurred for your company/organization?

	At primary data center	At a secondary data center	At a hosted/managed site	In our private cloud	In our public cloud	No loss occurred	Avg.
Lost one virtual machine	42.2%	13.3%	13.3%	11.1%	11.1%	8.9%	0.0
Lost one host machine	46.7%	13.3%	11.1%	2.2%	13.3%	13.3%	0.0
Lost one critical application	33.3%	15.6%	8.9%	20.0%	8.9%	13.3%	0.0
Lost multiple virtual machines	28.9%	15.6%	13.3%	8.9%	15.6%	17.8%	0.0
Lost multiple host machines	33.3%	20.0%	11.1%	6.7%	6.7%	22.2%	0.0
Lost multiple critical applications	31.1%	17.8%	17.8%	6.7%	15.6%	11.1%	0.0
Lost most or all of a data center	33.3%	13.3%	11.1%	8.9%	15.6%	17.8%	0.0

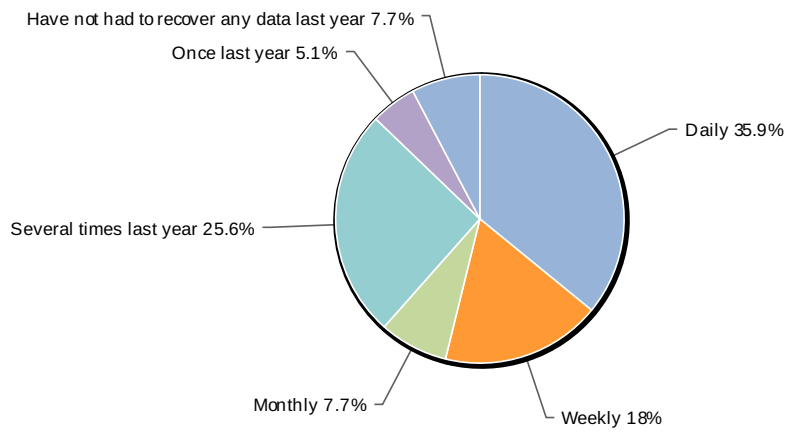
Lost most of all or a data center	22.2%	15.6%	13.3%	11.1%	13.3%	24.4%	0.0
Lost less than half overall storage	22.2%	11.1%	20.0%	11.1%	11.1%	24.4%	0.0
Lost more than half overall storage	17.8%	22.2%	6.7%	13.3%	11.1%	28.9%	0.0
Lost network connectivity	33.3%	15.6%	15.6%	13.3%	13.3%	8.9%	0.0
Lost critical data/files	31.1%	15.6%	24.4%	8.9%	0.0%	20.0%	0.0
Backups not recoverable	12.5%	16.7%	8.3%	29.2%	25.0%	8.3%	0.0
Replicas not recoverable	20.8%	16.7%	8.3%	20.8%	12.5%	20.8%	0.0
Archives not recoverable	4.2%	16.7%	20.8%	20.8%	20.8%	16.7%	0.0
Average %	28.7%	16.0%	13.9%	12.0%	12.0%	17.3%	0.0

When your company/organization experiences a loss in the data center, please describe the causes

	Most frequent cause	Frequently the cause	Sometimes the cause	Almost never the cause	Not applicable	Avg.
Security Breach	22.5%	27.5%	10.0%	20.0%	20.0%	0.0
Lack of documentation	25.0%	25.0%	25.0%	2.5%	22.5%	0.0
Human error	35.6%	26.7%	20.0%	6.7%	11.1%	0.0
Lack of training	28.9%	26.7%	20.0%	8.9%	15.6%	0.0
Lack of procedure/documentation	22.2%	24.4%	17.8%	11.1%	24.4%	0.0
Hardware failure	28.9%	20.0%	24.4%	11.1%	15.6%	0.0
Software failure	15.6%	26.7%	22.2%	13.3%	22.2%	0.0
Power failure	24.4%	22.2%	20.0%	20.0%	13.3%	0.0
Backup/restore failure	20.0%	11.1%	26.7%	20.0%	22.2%	0.0
Network failure/slowdown	24.4%	15.6%	22.2%	13.3%	24.4%	0.0
Building or physical infrastructure failure	22.2%	15.6%	35.6%	17.8%	8.9%	0.0
Failure of alerting or monitoring system	26.7%	17.8%	24.4%	15.6%	15.6%	0.0
Weather event	24.4%	17.8%	17.8%	22.2%	17.8%	0.0
Lack of capacity planning/foresight	20.0%	17.8%	24.4%	26.7%	11.1%	0.0
Deliberate attack from outside our company	24.4%	17.8%	20.0%	26.7%	11.1%	0.0
Deliberate attack from inside our company	28.9%	13.3%	17.8%	15.6%	24.4%	0.0
Slowdown or performance problem	25.0%	25.0%	12.5%	20.0%	17.5%	0.0
Average %	24.7%	20.5%	21.3%	16.0%	17.5%	0.0

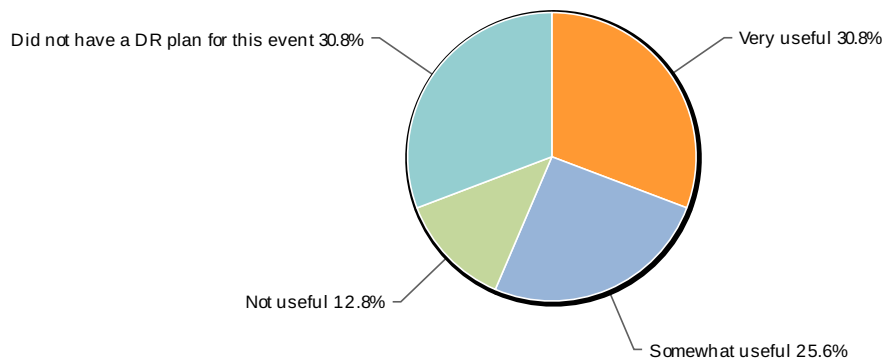
How often have you had to recover any data in the last year?

Value	Percent %
Daily	35.9%
Weekly	18.0%
Monthly	7.7%
Several times last year	25.6%
Once last year	5.1%
Have not had to recover any data last year	7.7%



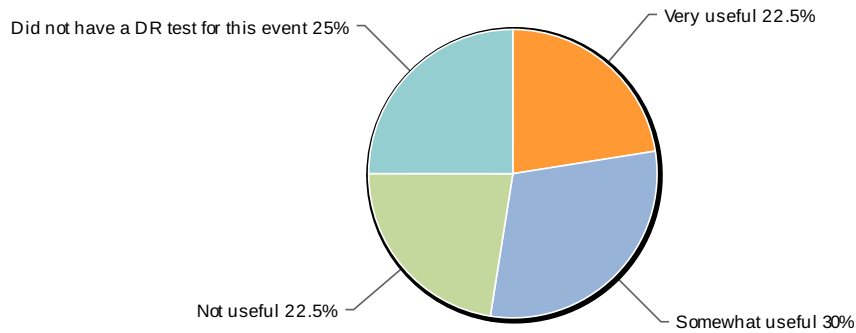
Did your DR plan prove useful for your worst DR event?

Value	Percent %
Very useful	30.8%
Somewhat useful	25.6%
Not useful	12.8%
Did not have a DR plan for this event	30.8%



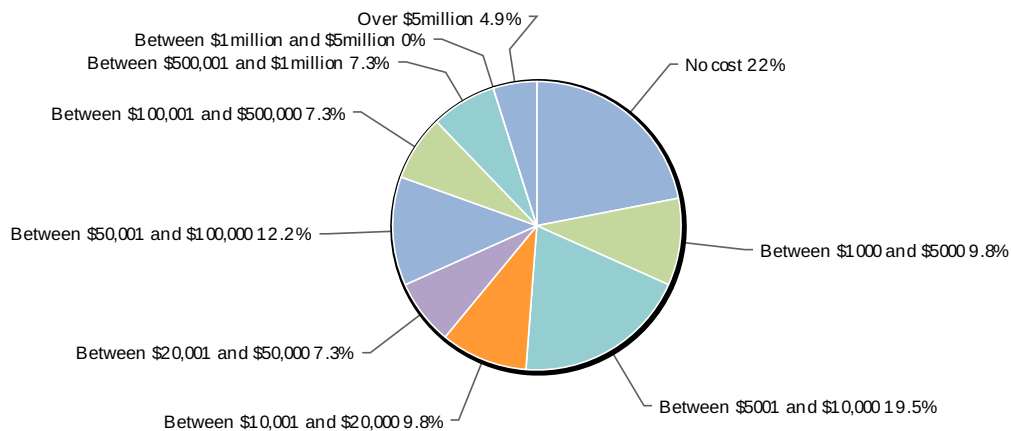
Did your DR Testing prove useful for your worst DR event?

Value	Percent %
Very useful	22.5%
Somewhat useful	30.0%
Not useful	22.5%
Did not have a DR test for this event	25.0%



Please estimate the total cost for recovery and business disruption of your worst loss or DR event.

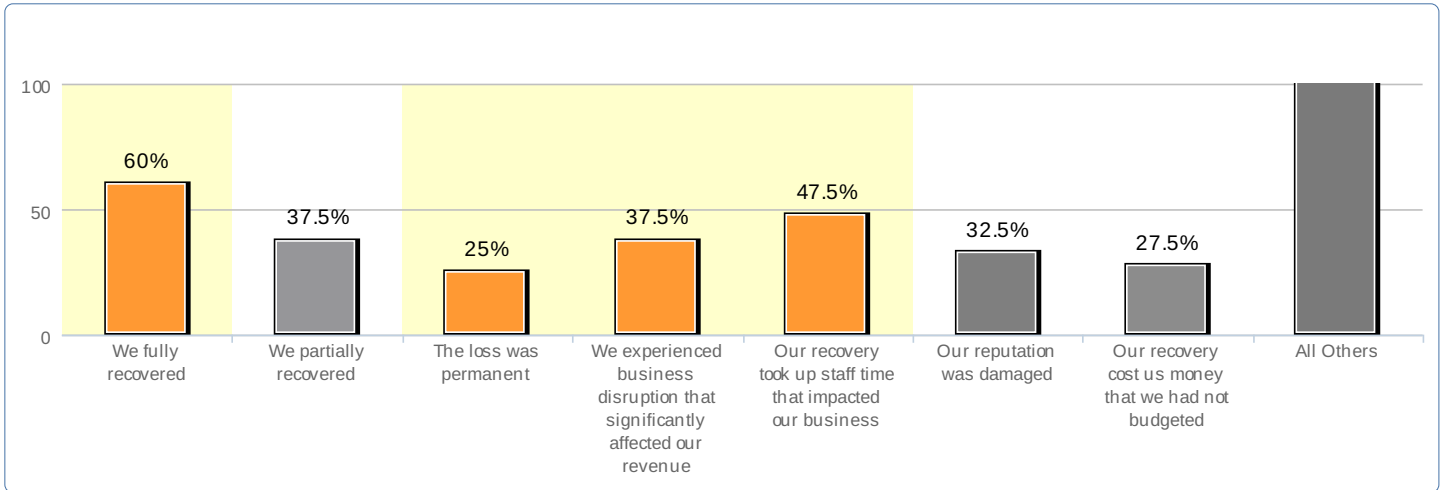
Value	Percent %
No cost	22.0%
Between \$1000 and \$5000	9.8%
Between \$5001 and \$10,000	19.5%
Between \$10,001 and \$20,000	9.8%
Between \$20,001 and \$50,000	7.3%
Between \$50,001 and \$100,000	12.2%
Between \$100,001 and \$500,000	7.3%
Between \$500,001 and \$1million	7.3%
Between \$1million and \$5million	0.0%
Over \$5million	4.9%



What were the effects of your worst loss or DR event? Check all that apply.

Value	Percent %
We fully recovered	60.0%
We partially recovered	37.5%
The loss was permanent	25.0%
We experienced business disruption that significantly affected our revenue	37.5%
Our recovery took up staff time that impacted our business	47.5%

Our reputation was damaged	32.5%
Our recovery cost us money that we had not budgeted	27.5%
Our disaster recovery plan was blamed for some or all of the incident	22.5%
Our disaster recovery plan was altered as a result of the incident	32.5%
Our IT staff or practices were altered as a result of the incident	35.0%
Our data center or disaster recovery budget was increased as a result of the incident	27.5%
Our data center configuration was altered as a result of the incident	17.5%
We changed our DR test plans	15.0%



You can compare your grade to the grades of others who took the benchmark:

- Over 119 points = "A"
- 103 to 118 points = "B"
- 87 to 102 points = "C"
- 71 to 86 points = "D"
- below 70 points = "F"

Your Disaster Preparedness Score:

Value	Percent %
32	2.2%
34	2.2%
38	2.2%
39	2.2%
40	2.2%
44	2.2%
45	2.2%
46	4.4%
47	2.2%
48	4.4%
49	2.2%
50	4.4%
52	2.2%
53	6.7%

Statistics	
Sum	2,568.0
Avg.	57.1
StdDev	12.2
Max	89.0

54	2.2%
55	2.2%
56	4.4%
57	2.2%
58	2.2%
59	2.2%
60	2.2%
62	4.4%
64	11.1%
65	2.2%
67	2.2%
70	6.7%
72	4.4%
73	2.2%
74	2.2%
80	2.2%
89	2.2%

