Symantec 2010 Disaster Recovery Study

Global Results

November 2010

CONTENTS

EXECUTIVE SUMMARY

The sixth annual Symantec Disaster Recovery Study demonstrates the challenges that data center managers have in managing disparate virtual, physical and cloud resources. These ever-changing resources add complexity for organizations protecting and recovering mission-critical applications and data. In fact, the data found virtual machines are not properly protected due to resource and other storage constraints that hamper backups.

The study also found a huge gap in terms of how fast they think they can recover and how fast they actually do. In addition, organizations still experience more downtime than they should from basic causes such as system upgrades, power outages and cyberattacks.
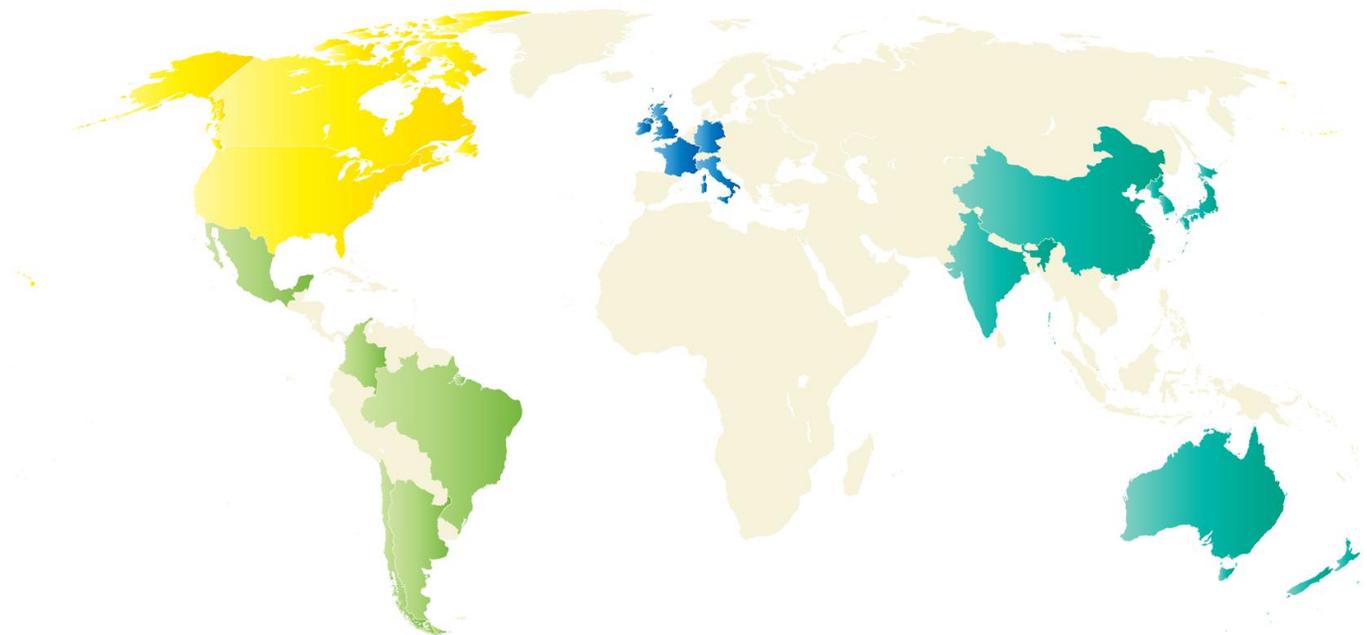
Finally, the study shows significant improvements in disaster recovery testing frequency; however disruption to employees, sales and revenue is still high.

METHODOLOGY

Applied Research performed a telephone survey in October 2010. The
survey included 1,700 enterprises with 5,000 employees or more from
18 countries worldwide. The survey covered a variety of industries.

The confidence level of this survey is 95 percent +/- 2.4 percent.

Additionally, Symantec held telephone focus groups with a range of IT
professionals, in order to gain deeper insight into their responses and
experiences.

North America	
United States	175
Canada	25

Latin America	
Brazil	75
Mexico	75
Argentina	20
Colombia	15
Chile	15

EMEA	
United Kingdom	100
Italy	100
France	100
Germany	100

APJ	
Australia	90
New Zealand	60
India	150
China	300
Japan	100
Korea	100
Singapore	100

Symantec.

FINDING 1:
## Virtualization and cloud make DR complex

The ever-increasing amount of applications and data that reside in virtual and cloud environments is difficult for data center managers to protect, control and manage. The data shows that the added complexities of these environments cause them not to be protected as well as they could be.
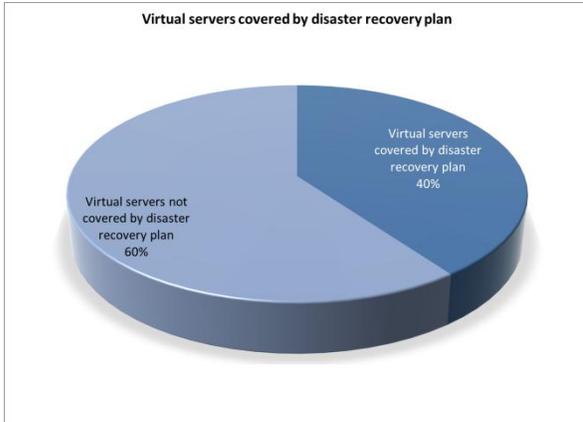
Respondents report that between one-fourth and one-third of all applications are in virtual environments. Eighty-four percent of respondents say that virtualization has led them to reevaluate their DR plans.

However, even though more applications and data are in virtual environments, 60 percent of virtualized servers are not covered in current DR plans. Symantec also found that a little more than half (56 percent) of the data on virtual systems is regularly backed up. Eighty-two percent of backups occur only weekly or less frequently, rather than daily.

Symantec believes that the growth of virtual servers, server sprawl and lack of tools may be the reason for these changes.
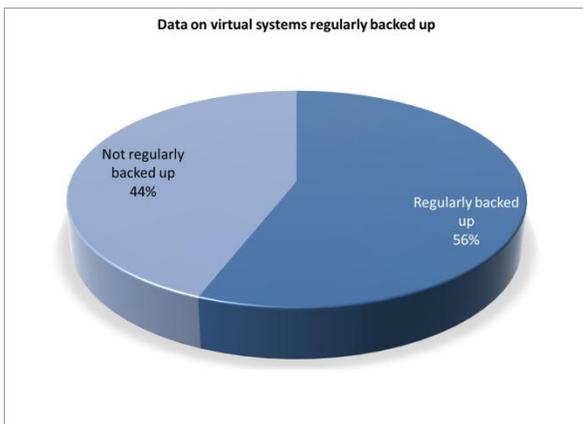
Furthermore, Respondents indicated that 20 percent of their organization's data and mission-critical applications in virtual environments are protected by replication. Respondents indicated that the same amount of data is protected by both high availability failover and global/wide area failover.
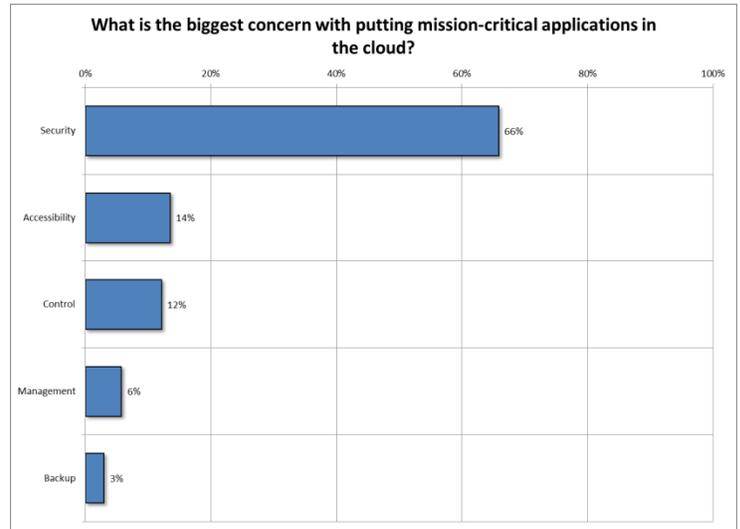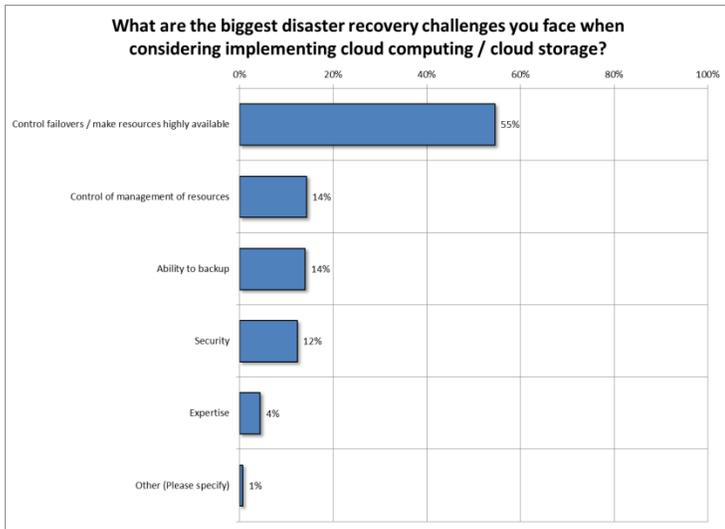
In focus groups, respondents said that replication technologies were one item that organizations often cut corners in implementing. One data manager said, "Here, we lack replication. It was something that we were going to implement, and due to company changes, our replication plan fell by the wayside. So, it's something that, when we talk about disaster recovery, we kind of grit our teeth and go, yes, we live in California, and yes, we're going to have an earthquake, and yes, we've got our tapes in another building, but we'd really love to have them in another city. And we lack that at this point."

Organizations also use the cloud for approximately half of both their mission-critical applications and their non-mission-critical applications; however, the lack of control of cloud environments is an issue. Organizations need better tools to manage virtual and cloud environments.

Virtual servers covered by disaster recovery plan

Virtual servers covered by disaster recovery plan
40%

Virtual servers not covered by disaster recovery plan
60%

Data on virtual systems regularly backed up

Not regularly backed up
44%

Regularly backed up
56%

While security is the main *concern* of putting applications into the cloud as reported by two thirds (66 percent) of respondents, the biggest disaster recovery *challenge* respondents say they face when considering implementing cloud computing / cloud storage is the ability to control failovers and making resources available (55 percent).

Keeping up with different tools that manage and protect these applications is a challenge for organizations, especially with the increase of applications and data that reside in virtual and cloud environments.

A data center manager for a manufacturer in the automotive sector in California stated, "If I knew of a tool that would do everything for us, I'd be happy to take a look at it."

What are the biggest disaster recovery challenges you face when considering implementing cloud computing / cloud storage?

Control failovers / make resources highly available	55%
Control of management of resources	14%
Ability to backup	14%
Security	12%
Expertise	4%
Other (Please specify)	1%

What is the biggest concern with putting mission-critical applications in the cloud?

Security	66%
Accessibility	14%
Control	12%
Management	6%
Backup	3%

FINDING 2:
The downtime recovery gap

There is an old adage that says that any IT project will take you at least twice as long as you think. When it comes to how long it takes for organizations to recover from downtime, the study found this to be true.

There is a major disconnect in terms of how long it actually takes to recover from an outage and how long organizations think it should take. When asked how long it would take them to recover if a significant disaster were to occur that destroyed their main data center, respondents indicated that it would take just over two hours to be up and running. However, respondents reported that in the past 12 months, the average amount of downtime per incident was 5 hours.

Part of this is likely due to unaccounted needs that arise during an outage. One data center manager reported, "I think a lot of companies, when the disaster hits, are going to be so overwhelmed. And their first priority would be catering to emergency services – fire departments, hospitals, and all that. So, I don't know how many of us would be in the same boat, but I think it's going to affect us considerably."

System upgrades (72 percent) are the largest cause of downtime for organizations in the past five years. Organizations also experienced an average of 50.9 hours of downtime from system upgrades, making it one of the largest causes of downtime as measured by both hours of downtime and number of incidents.

Referring to one way system upgrades impact DR testing, a data center manager said, "We have a number of upgrades scheduled over the next three months, and at some point during those three months, or even after the upgrades are complete, I can't guarantee that the systems are all going to function in the exact same way that they do today, because there's a lot of things that are changing."

Power outages and failures (70 percent) was the second greatest cause of downtime. Considering how many organizations cited power outages and failures as one of the leading causes of downtime, it is surprising that only 26 percent of organizations have conducted a power outage and failure impact assessment.
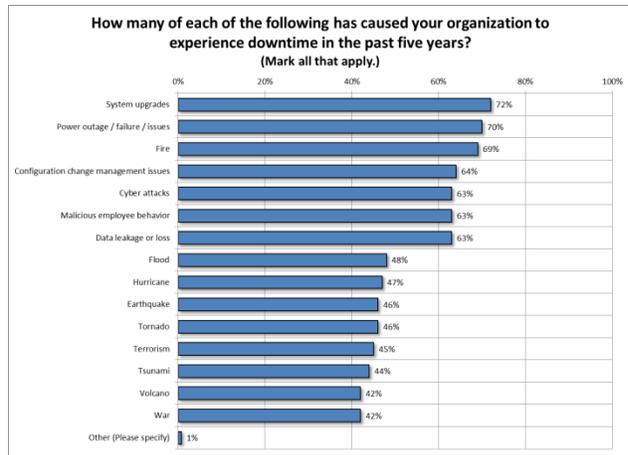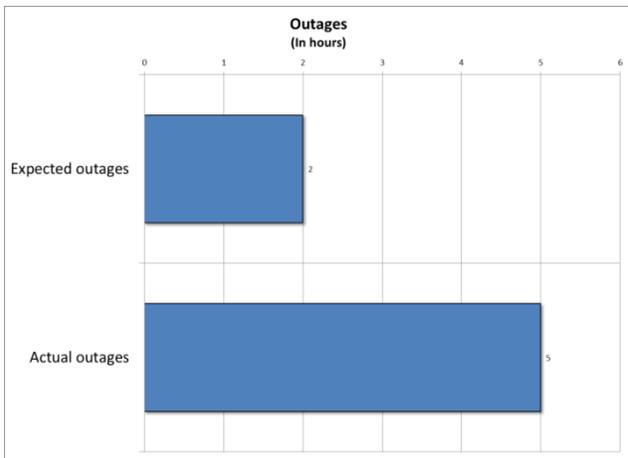
FINDING 3:
Impact of disaster recovery testing

The study also shows significant improvements in disaster recovery testing frequency; however disruption to employees, sales and revenue is still high.
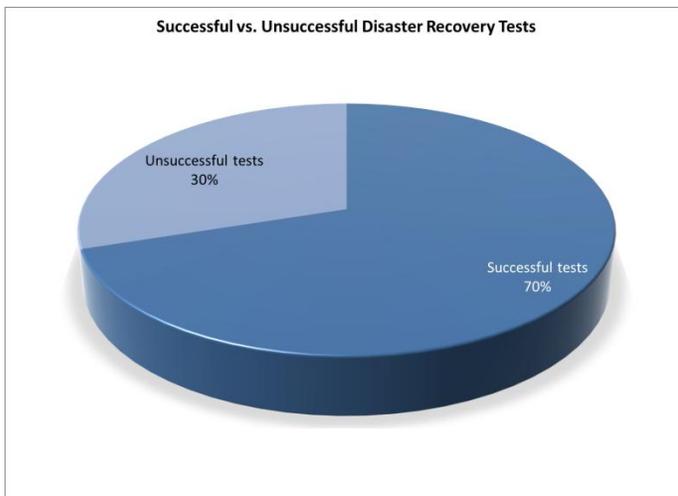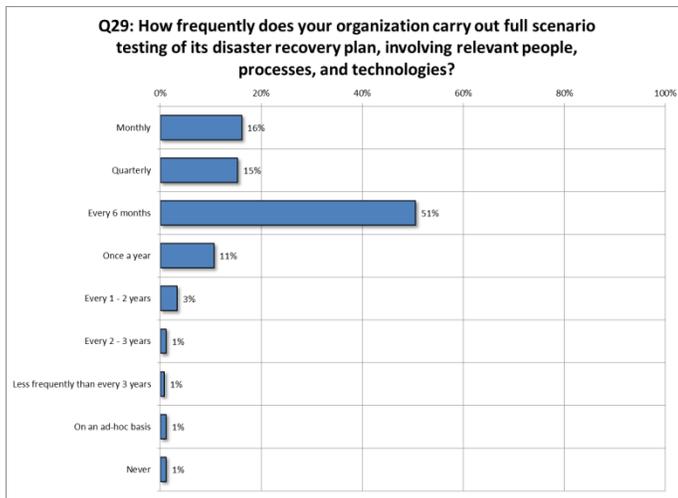
Respondents report that more than one-fourth (26 percent) of the total annual IT budget goes to DR-related initiatives, and is seen as part of the basic infrastructure of doing business. In terms of budget, organizations spent an average of $606,948 on DR testing in the past 12 months.

One data center manager for a manufacturer in the automotive sector in California said, "Disaster recovery is going to be an expense that's necessary to keep your business contingents going. It's just a cost of doing business."

Symantec has seen improvement in the number of organizations that test their DR plans more frequently. Approximately 82 percent of organizations test their DR plans either once a year or more frequently. This is a significant increase from the 66 percent from last year's study.

Forty percent of disaster recovery tests failed to recover critical data and applications within RTOs / RPOs. Of those that failed, organizations primarily blame inadequate IT infrastructure at the DR site.

The reasons most cited for why organizations are not testing more include the following: resources, in terms of budget (60 percent); disruption to employees (59 percent); disruption to customers / disruption to sales and the revenue stream (24 percent); and resources, in terms of people's time (26 percent).

Q29: How frequently does your organization carry out full scenario testing of its disaster recovery plan, involving relevant people, processes, and technologies?

Category	Percentage
Monthly	16%
Quarterly	15%
Every 6 months	51%
Once a year	11%
Every 1 - 2 years	3%
Every 2 - 3 years	1%
Less frequently than every 3 years	1%
On an ad-hoc basis	1%
Never	1%

Successful vs. Unsuccessful Disaster Recovery Tests

Unsuccessful tests 30%

Successful tests 70%

Symantec

SYMANTEC'S RECOMMENDATIONS

- **Treat all environments the same:** Ensure that mission-critical data and applications are treated the same across environments (virtual, cloud, physical) in terms of DR assessments and planning
- **Use integrated tool sets:** By using fewer tools that manage physical, virtual and cloud environments it will help organizations save time, training costs and help them to better automate processes
- **Simplify data protection processes:** Embrace low-impact backup methods and deduplication to ensure that mission-critical data in virtual environments is backed up, efficiently replicated off campus
- **Plan and automate to minimize downtime:** Prioritize planning activities and tools that automate and perform processes which minimize downtime during system upgrades
- **Identify issues earlier:** Implement solutions that detect issues, reduce downtime and recover faster to be more in line with expectations
- **Don't cut corners:** Organizations should implement basic technologies and processes that protect in case of an outage, and not take shortcuts that will have disastrous consequences.