



2008 Disaster Recovery Research Overview and Key Findings

Research Overview

- The Symantec sponsored 2008 Disaster Recovery Research report highlights business trends regarding disaster planning and preparedness.
- As the fourth year of this annual global survey, the report provides insight and understanding into some of the more complicated factors associated with disaster recovery.

Overview of Findings:

- Although one third of organizations have had to execute a disaster recovery plan, just under half say they can get fully operational in a week.
- The amount of applications that IT Managers believe are business critical has increased 20 percentage points over data from the previous year, and only about half of these applications are covered in DR plans.
- Virtualization is driving organizations to reevaluate their DR plans.
- Organizations report that DR testing impacts customers, sales and revenue because of the lack of tools that can address both virtual and physical environments.
- Despite increasing importance of DR, there is an alarming decrease in executive involvement. Executive complacency could be attributed to the improvement in DR testing successes.

Key Stats:

Virtualization

Virtualization is causing organizations to re-evaluate their DR plans. More automated and cross platform, cross environment tools are needed.

- Virtualization is causing 55 percent of organizations worldwide to reevaluate their DR plans (this varies by region):
 - Virtualization has caused only 69 percent of organizations in South America to reevaluate their plans
 - Virtualization has caused only 64 percent of organizations in North America to reevaluate their plans
 - Virtualization has caused only 52 percent of organizations in Asia Pacific to reevaluate their plans
 - Virtualization has caused only 43 percent of organizations in EMEA to reevaluate their plans
- Fifty-four percent of respondents listed resource constraints as their top challenge with backing up virtual systems, which indicates a need for simplified and automated tools.
- Thirty-five percent of virtual servers are not covered in organizations' DR plans.
- Only 37 percent of respondents report they back up more than 90 percent of their virtual systems.
- Globally, 35 percent of respondents cited 'too many different tools' as the biggest challenge in protecting mission-critical data and applications within physical and virtual environments. Second and third are 'lack of automated recovery tools' and 'insufficient backup tools', each with 33 percent.

- In North America: Nearly half (44 percent) of respondents report that too many different tools for physical and virtual environments is the biggest challenge in protecting mission critical data and applications in virtual environments. Second is a lack automated recovery tools (41 percent), followed closely by insufficient back up tools (39 percent).

Success of testing or recovery

More than one third of organizations have had to execute their DR plans. More than half don't think they will be up and running fully in one week if they had to execute their plans. A third of tests don't meet RTOs.

- Of organizations that have had to execute their DR plans, the top reasons include:
 - Computer system failure (i.e. hardware and software) 36 percent
 - External computer threats (i.e. viruses and hackers) 28 percent
 - Power outage/failure/issues – 26 percent
 - Natural disasters, IT problem management, Data leakage or loss and internal computer threats (accidental and malicious employee behavior follows closely at 23 percent, 23 percent, 22 percent and 21 percent, respectively.
- For the tier-one applications in a disaster recovery plan, respondents report that their recovery time objectives are 30 hours.
- Only 30 percent of tests meet RTO objectives.
- Only 31 percent of respondents reported that they could achieve baseline operations within one day if a significant disaster occurred that obliterated their main data center. Only 3 percent believed they have skeleton operations within 12 hours.
- Forty-seven percent believed they could have 100 percent normal operations within one week.

Scope of DR Plans

There is less involvement by executives in DR planning and testing. In addition, the amount of applications deemed critical rose significantly year over year. However, only around half of those critical applications, databases and email are covered in DR plans.

- In the 2007 DR survey, 55 percent of respondents said that their DR committees involved the CIO / CTO / IT director. In 2008, that number drops to 33 percent worldwide.
- Although 56 percent of applications were deemed mission critical by respondents, only 54 percent of applications are covered by DR plans.
- In 2007, 36 percent of applications were deemed mission critical, showing a 20 percentage point increase.
- 55 percent of organizations include web servers in their DR plans, and 54 percent include databases and applications.
- Only 50 percent of respondents include email in their DR plans.
- Only 43 percent respondents say remote offices are covered in organizations' DR plan.
- South America leads the way in DR planning. 60 percent of databases, 53 percent of applications, and 51 percent of email and 67 percent of web servers are covered by DR plans.

Impact on business

More organizations are testing their DR plans in 2008 and there is significantly less failure in tests. However, the impact of DR testing on the business is significant.

- Approximately 47 percent of organizations test their DR plans either once a year or less than once a year.

- Asia and EMEA are less likely to test their DR plans, with 12 percent of respondents in EMEA and 8 percent in Asia Pacific reporting that they never test their DR plans. Only 2 percent of North and South American organizations never test.
- 93 percent of IT organizations report that they have tested their disaster recovery plans at least once, yet they report that 30 percent of tests fail.
- Only 16 percent say that tests have never failed.
- In 2007, this report showed that 91 percent of IT organizations test their disaster recovery plans, yet 50 percent of those tests failed. There is some improvement being made in the industry with respect to successful DR testing.
- While there are apparently improvement in the percentage of successful tests, one-third (32 percent) of organizations report that disaster recovery testing will impact their customers, and one-fifth (21 percent) admit such testing could impact their organization's sales and revenue.
- Reasons cited for why organizations don't do more testing include: lack of resources in terms of people's time (39 percent), disruption to employees (39 percent), budget (37 percent) and disruption to customers (32 percent). In addition, 21 percent admit they don't test because DR testing could significantly disrupt sales and revenue.
- Reasons reported for tests failing include: People do not do as they are supposed to (35 percent); technology doesn't do what it is supposed to (29 percent); insufficient IT infrastructure at DR site (25 percent); followed by out of date plans (24 percent) and inappropriate processes (23 percent).
- In 2007, 88 percent of IT professionals polled carried out a probability and impact assessment for at least one threat, in 2008, 98 percent of respondents indicated they had carried out an assessment for at least one threat.

Survey Methodology/Demographics

- Symantec commissioned a survey through Applied Research of a total of 1000 respondents from 15 countries.
- Survey respondents include IT managers and C-level decision makers responsible for DR plans working in organizations with 500 or more employees that have a DR plan in place.
- Surveys were conducted via phone and results reflect global findings.
- Geographic areas included North America, Asia Pacific, EMEA and Latin America. Specific countries include:
 - United States
 - Canada
 - United Kingdom
 - Japan
 - Germany
 - China
 - India
 - Australia
 - France
 - Singapore
 - Malaysia
 - Italy
 - Brazil
 - Mexico
 - Korea

###