



2009 Disaster Recovery Research Key Findings

Research Overview

- The Symantec-sponsored 2009 Disaster Recovery Research report highlights current business trends regarding disaster planning and preparedness.
- As the fifth year of this global survey, the report provides insight and understanding into some of the more complicated factors associated with disaster recovery.

Key Findings

Impact of downtime on business

Nearly all organizations have had to use their DR plans, from which it takes about four hours to get back up and running on average in the past year, and cost an average of nearly \$300,000. However, these figures are dramatically improved from 2008 numbers. As IT becomes a more critical business function, the business requirements for IT service and information available are increasing in terms of RTOs/RPOs.

- Sixty percent of applications were deemed mission critical by respondents, and nearly the same amount is covered in DR plans. In 2008, 56 percent of applications were deemed mission critical by respondents. Any sort of outage of these systems will have an enormous impact to the business.
- In fact, 93 percent of organizations have had to execute on their disaster recovery plans.
- In general, respondents report that it takes about three hours to achieve skeleton operations after an outage, and four hours to be up and running after an outage.
- This is dramatically improved over the 2008 findings, where only 31 percent of respondents reported that they could achieve baseline operations within one day if a significant disaster occurred at their main data center, and only 3 percent believed they would have skeleton operations within 12 hours.
- The average cost of executing/implementing disaster recovery plans for each downtime incident worldwide according to respondents is US\$287,600. The median cost of executing/implementing disaster recovery plans for each downtime incident worldwide ranges from approximately \$100,000 to \$500,000 (half a million dollars). In North America, the median cost can climb to as high as \$900,000. Globally, this number is highest for healthcare and financial services organizations. In North America, the median cost for financial institutions is \$650,000.

Impact of executive involvement

Recovery time objectives fell over the past year. Although DR budgets continue to rise in 2009 it is expected to be flat in 2010. Because of this and other factors, executive involvement has significantly increased from last year. The rate of successful DR testing is also improving.

- The annual budget for disaster recovery initiatives is 50 million (this includes backup, recovery, clustering, archiving, spare servers, replication, tape, services, DR plan development and offsite costs). According to respondents, this number continues to grow in 2009.

- More than half (52 percent) of respondents report that this number will be flat in 2010. And, 42 percent believe their disaster recovery budgets will increase during the same time period.
- In the 2007 DR survey, 55 percent of respondents said that their DR committees involved the CIO / CTO / IT director. In 2008, that number dropped to 33 percent worldwide. In 2009, this number increased upward to 70 percent.
- Symantec believes that some of this increase from previous years and attention on DR may be due to DR becoming a competitive differentiator, as well also a number of other factors including the size of DR budgets and the impact on customers of downtime that leads executives to focus more on keeping existing processes running smoothly.
- Mirroring this growth of executive involvement we see lower RTOs/RPOs.
- Recovery time objectives fell from median of 5 hours in 2008 to 4 hours in 2009.
- The survey also demonstrated that DR testing was less likely to fail than in previous years. In 2009, 75 percent of tests were successful, more than doubling the 30 percent of tests that met RTO objectives in 2008. While this rate also parallels executive involvement, they may or may not be correlated.

Impact of testing on business

More organizations are testing their DR plans and meeting their objectives in 2009 than in previous years, however, the impact on customers, revenue and internal clients is much higher than ever before. In addition, one of four tests fails. Lack of resources continues to be an issue, and automation can help address much of the existing issues. Symantec believes DR testing is invaluable, but also that organizations shouldn't let DR testing cause significant downtime. Rather organizations should look to implement testing methods which are non-disruptive.

- Approximately 35 percent of organizations only test their DR plans either once a year or less than once a year. This is 12 percent lower (and an improvement) from the 47 percent that reported minimal testing in 2008. However, Symantec and most IT experts believe that every organization should be testing more frequently than once a year.
- Ninety-six percent of IT organizations report that they have tested their disaster recovery plans at least once, up from 93 percent in 2008.
- Respondents report that 25 percent of their DR tests failed, down from 30 percent in 2008, and 50 percent in 2007). Only 15 percent say that tests have never failed. Although this is good news, one test failure in four is still alarmingly high.
- While there is improvement in the percentage of successful tests, testing increasingly impacts customers and revenue. Forty percent of respondents report that disaster recovery testing will impact their customers (up from 32 percent in 2008) and nearly one third (27 percent) report that such testing could impact their organization's sales and revenue (up from one fifth or 21 percent in 2008).
- The reasons most cited for why organizations don't do more testing include: lack of resources in terms of people's time (48 percent), disruption to employees (44 percent), budget (44 percent) and disruption to customers (40 percent).
- In addition, Symantec believes that organizations shouldn't let DR testing cause significant downtime. Rather organizations should look to implement testing methods which are non-disruptive.
- Reasons reported for tests failing include: People do not do as they are supposed to (47 percent); technology doesn't do what it is supposed to (40 percent); inappropriate processes (37 percent); and out of date plans (35 percent). Insufficient technology dropped from third to fifth on the list from last year at 23 percent.
- Symantec believes that the main reasons that tests don't succeed – people and processes don't work as they were supposed to in nearly half of the cases – point to the need for more automation.

Impact of virtualization

Virtualization is causing organizations to re-evaluate their DR plans. Still, nearly a third of organizations don't test virtual environments as part of their DR plans, and the same amount of virtual environments is not regularly backed up. More automated and cross platform, cross environment tools are needed.

- Virtualization has caused 64 percent of organizations worldwide to reevaluate their DR plans. This is up from 55 percent in 2008.
- One-fifth of databases, application servers and web servers are currently virtualized. Yet, only 55 percent of virtual servers are covered by organizations' disaster recovery plans.
- Almost two thirds (59 percent) of organizations are using disk backup to protect their data and critical applications in virtual environments.
- Nearly a third of respondents (27 percent) don't test virtual servers as part of their disaster recovery plans. This is down from 35 percent in 2008.
- More than one-third (36 percent) of data on virtualized systems is not regularly backed up.
- Fifty-one percent of respondents listed resource constraints as their top challenge with backing up virtual systems, which indicates a need for simplified and automated tools.
- Globally, 53 percent of respondents cited lack of storage management tools as the top challenge in protecting mission critical data and applications in virtual environments. Lack of backup storage capacity (52 percent) and lack of automated recovery tools (50 percent) both came in a close second.
- This differs from last year's results where 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. Lack of automated recovery and insufficient backup tools came in close second, each with 33 percent.

Survey Methodology/Demographics

- Symantec commissioned a survey through Applied Research of a total of 1650 respondents from 24 countries.
- Survey respondents include IT managers and C-level decision makers responsible for DR plans working in organizations with 5000 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, EMEA, Asia Pacific and Latin America.
Specific countries include:
 - United States
 - Canada
 - United Kingdom
 - France
 - Germany
 - Italy
 - Hungary
 - Nigeria
 - UAE
 - KSA
 - Russia
 - South Africa
 - Turkey
 - Spain
 - China
 - Japan
 - India
 - Australia
 - Singapore
 - Malaysia
 - Korea
 - New Zealand
 - Brazil
 - Mexico

###