

# Symantec Corp. (Nasdaq: SYMC) global results of its fifth Disaster Recovery survey, which demonstrates rising DR pressures on organisations caused by soaring downtime costs and more stringent IT service level requirements to mitigate risk to the business.

01 July, 2009 11:03:00

Symantec research reveals IT spending more on DR yet vulnerable in testing, virtual environment

SYDNEY, Australia – July 1, 2009 – Symantec Corp. (Nasdaq: SYMC) today announced the global results of its fifth Disaster Recovery survey, which demonstrates rising DR pressures on organisations caused by soaring downtime costs and more stringent IT service level requirements to mitigate risk to the business. The study also shows that while DR budgets are higher in 2009, they are expected to remain flat over the next few years – requiring IT professionals to do more with the same or less.

The survey highlights that while recovery time objectives were reduced to less than 4 hours in 2009, disaster recovery testing and virtualisation are still major challenges for organisations. Respondents report that DR testing increasingly impacts customers and revenue, and one in four tests fail. Nearly a third of organisations don't test virtual environments as part of their disaster recovery plans, and a slightly larger percentage of virtual environments aren't regularly backed up – pointing to the need for more automation and cross-environment tools.

## **Downtime costs are significant**

The average cost of executing/implementing disaster recovery plans for each downtime incident worldwide according to respondents is US \$287,600. In Australia and New Zealand, the median cost was USD\$570,000 compared to USD\$900,000 in North America. Globally, this number is highest for healthcare and financial services organisations.

This is alarming when one considers that one in four tests failed and 93 per cent of organisations have had to execute on their disaster recovery plans. Respondents reported that it takes on average three hours to achieve skeleton operations after an outage, and four hours to be up and running. This is dramatically improved over the 2008 findings, where only three per cent of respondents reported that they could achieve skeleton operations within 12 hours, and 31 per cent believed they would have baseline operations within one day.

## **2009 DR spending bucks trend**

The research shows that the annual median budget for disaster recovery initiatives, including backup, recovery, clustering, archiving, spare servers, replication, tape, services, disaster recovery plan development and offsite costs at data centres surveyed is \$50 million. According to respondents, this number will continue to grow throughout 2009, but more than half (52 per cent globally and 55 per cent in Australia and New Zealand) of respondents believe that budgets will be flat in 2010, making it more challenging for IT management to better leverage their assets including hardware, software and personnel.

## **Executive involvement doubled in past year**

According to the 2009 disaster recovery survey, 70 per cent (66 per cent in Australia and New Zealand) of respondents reported that their disaster recovery committees involved the CIO, CTO or IT director – a significant increase from last year's research where 33 per cent of respondents indicated executive involvement. As budgets increased over the past year, disaster recovery initiatives have become more of a competitive differentiator, and impact of downtime on customers is greater than ever. Another reason for executive involvement is the increase of applications that are seen as mission critical. Sixty per cent of applications globally and 55 per cent in Australia and New Zealand were deemed mission critical by respondents, and nearly the same amount (61 per cent in

Australia and New Zealand) is covered in disaster recovery plans. Any sort of outage to these systems will have an enormous impact to the business.

#### Disaster recovery testing improves but still a major challenge

This year, 35 per cent of respondents globally and 39 per cent in Australia and New Zealand reported that they test their DR plans once per year or less frequently – a 12 per cent improvement globally (21 per cent improvement in Australia and New Zealand) from last year. In addition, one in four tests still fail, showing a dramatic need for improvement in this area. Reasons most respondents cited for why organisations aren't testing include:

Lack of resources in terms of people's time (48 per cent globally and 40 per cent in Australia and New Zealand)

Disruption to employees (44 per cent globally and 41 per cent in Australia and New Zealand)

Budget (44 per cent globally and in Australia and New Zealand)

Disruption to customers (40 per cent globally and 39 per cent in Australia and New Zealand)

Also a concern is that more organisations reported that disaster recovery testing increasingly impacts customers and revenue over previous years. Forty per cent of respondents globally and 39 per cent in Australia and New Zealand reported that disaster recovery testing will impact their organisations' customers and nearly one third (27 per cent globally and in Australia and New Zealand) reported that such testing could impact their organisation's sales and revenue (up from one fifth or 21 per cent globally and 12 per cent in ANZ in 2008). Symantec recommends that organisations implement disaster recovery testing methods that can be run frequently and without disruption to business operations. Symantec believes that people and processes are the main reason tests fail, pointing to the need for more automation.

#### Virtualisation still a major challenge

Sixty-four per cent of worldwide respondents and 59 per cent in Australia and New Zealand reported that virtualisation is causing them to reevaluate their disaster recovery plans. This is up from 55 per cent globally and 44 per cent in Australia and New Zealand in 2008. Still, nearly a third (27 per cent globally and 35 per cent in Australia and New Zealand) of organisations do not test virtual environments as part of their disaster recovery initiatives. This number has improved in the past year, lowering from more than one-third (35 per cent) of organisations who did not test in 2008. Additionally, more than one-third (36 per cent) of data on virtualised systems is not regularly backed up, showing no improvement in the past year (37 per cent in 2008). Over half of the respondents cited lack of backup storage capacity and automated recovery tools as top challenges to protecting data in virtual environments.

In addition, the study found that globally, more than half of respondents cited:

Lack of storage management tools as the top challenge in protecting mission critical data and applications in virtual environments (53 per cent globally and 51 per cent in Australia and New Zealand).

Lack of backup storage capacity (52 per cent globally and 39 per cent in ANZ) and lack of automated recovery tools (50 per cent globally and 49 per cent in ANZ) both came in a close second globally. Within ANZ, lack of automated recovery (49 per cent); insufficient backup tools (42 per cent in 2008; 14 per cent in 2009); lack of available backup and storage capacity (39 per cent); and different tools for physical and virtual environments (39 per cent in 2009; 28 per cent in 2008) were also cited as key challenges to protecting mission critical data and applications in virtual environments.

Resource constraints such as people, budget, and space as the top challenges to backing up virtual machines suggesting a need for greater automation and the ability to leverage existing IT investments in order to lower costs.

## **Recommendations**

As demonstrated over multiple years of this study, lack of resources continues to be an issue, yet the costs of downtime are staggering. Organisations can also do a better job at curbing the costs of downtime by implementing more automation tools that minimise human involvement and address other weaknesses in their disaster recovery plans.

Because disaster recovery testing is invaluable, but can significantly impact business – including customers and revenue – organisations should seek to improve the success of testing by evaluating and implementing testing methods which are non-disruptive.

Finally, organisations should include those responsible for virtualisation into disaster recovery plans, especially testing and backup initiatives. Virtual environments should be treated the same as a physical server, showing the need for organisations to adopt more cross-platform and cross-environment tools, or standardising on fewer platforms.

“This year’s Symantec-sponsored research clearly identifies key issues, hidden risks and best practices in implementing disaster recovery plans. While some aspects are trending well, the impact of downtime is greater than ever before,” said Rob Soderbery, senior vice president of Symantec’s Storage and Availability Management Group. “The surging cost of downtime places greater emphasis on business – which means more pressure on IT. If organisations are not protecting virtual environments, not testing their disaster recovery plans and seeing one out every four tests fail then something needs to change to better manage risk to the business. Organisations should implement solutions that address these needs while allowing them to leverage existing assets.”

## **About the 2009 Symantec Disaster Recovery Research Report**

In its fifth year, the 2009 Symantec Disaster Recovery Research report is an annual global study commissioned by Symantec to highlight business trends regarding disaster recovery planning and preparedness. Conducted by independent market research firm Applied Research West during June 2009, the study polled more than 1650 IT managers in large organisations across 24 countries in the U.S. and Canada, Europe and the Middle East, Asia Pacific and South America to gain insight and understanding into some of the more complicated factors associated with disaster recovery.

## **About Symantec**

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at [www.symantec.com](http://www.symantec.com).

###

NOTE TO EDITORS: If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at <http://www.symantec.com/news>. All prices noted are in U.S. dollars and are valid only in the United States.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.