



**PER ULTERIORI INFORMAZIONI CONTATTARE:**

Emanuela Lombardo

Symantec Italia

02/241151

emanuela\_lombardo@symantec.com

Francesco Petrella – Nadia Lauria – Elisabetta Giuliano -  
Rosaria Callea

Pleon

02/0066290

[francesco.petrella@pleon.com](mailto:francesco.petrella@pleon.com), [nadia.lauria@pleon.com](mailto:nadia.lauria@pleon.com),  
[elisabetta.giuliano@pleon.com](mailto:elisabetta.giuliano@pleon.com), [rosaria.callea@pleon.com](mailto:rosaria.callea@pleon.com)

**Vulnerabilita' nei test e negli ambienti virtuali: le sfide del Disaster Recovery in Italia secondo Symantec**

*Il Symantec Disaster Recovery Research Report 2009 evidenzia in Italia uno stallo della spesa IT nelle soluzioni di DR, nonostante la necessità di miglioramenti negli ambienti virtuali e nei test*

**Cupertino, Calif. – 20 luglio 2009** - Symantec Corp. (Nasdaq: SYMC) ha annunciato i risultati della quinta edizione dello studio "IT Disaster Recovery" da cui è emersa una crescente pressione nei confronti delle organizzazioni dovuta all'aumento dei costi legati al downtime e ai più rigidi requisiti di Service Level stabiliti per mitigare il rischio aziendale. Lo studio ha inoltre messo in luce come i budget DR (Disaster Recovery) siano destinati a non sperimentare alcun incremento per i prossimi anni, mettendo pertanto i professionisti IT nelle condizioni di dover ottenere di più con risorse uguali o inferiori.

La ricerca, che ha coinvolto oltre 1.650 IT manager di grandi aziende – 50 in Italia - ha rivelato che, a livello globale, i test e la virtualizzazione continuano a rappresentare in questo campo una delle maggiori sfide per le imprese. Secondo gli intervistati i test delle strategie DR producono un impatto sempre più forte su clienti e fatturato, e un test su quattro fallisce. Un terzo circa dei programmi di disaster recovery delle imprese non prevede test sugli ambienti virtuali; una percentuale di ambienti virtuali di poco superiore non risulta disporre di un sistema di backup regolare– mettendo in luce il bisogno di più strumenti di automazione capaci di funzionare attraverso tutti i vari ambienti.

**La situazione in Italia**

La ricerca di Symantec fotografa uno scenario italiano che rispecchia le tendenze globali: per gli intervistati italiani gli attacchi dei virus ( 64%) e i disastri naturali ( 48%) sono le principali cause che spingono le aziende a creare una strategia di Disaster Recovery, mentre web server ( 60%) e i database servers ( 50%) sono le principali tecnologie aziendali attualmente coperte da un piano di Disaster Recovery, seguite dalle applicazioni, come ad esempio l'ERP (48%) e dalle email ( 40%).

**Ingenti costi legati al downtime**

Secondo i risultati del sondaggio, in Italia il costo per l'esecuzione o l'implementazione di un piano di disaster recovery per ciascun caso di downtime ammonta a circa 65.000 dollari.

Un dato preoccupante se si considera che un test su quattro fallisce e che la quasi totalità delle imprese si è trovata a dover mettere in atto il proprio piano di disaster recovery. Gli intervistati hanno riferito che il tempo medio impiegato per ripristinare le attività aziendali di base a seguito di un caso di interruzione del servizio è di circa cinque ore, che salgono a sei per ritornare a una situazione di completa normalità e produttività.

### **Tendenze della spesa per DR nel 2010**

Lo studio dimostra come le decisioni delle imprese italiane sugli investimenti in DR sono molto diversificate. Le nostre aziende infatti si distribuiscono con un peso specifico identico ( 23%), tra quattro fasce di investimento ( < 1M\$, 1-25M\$, 25-50M\$, 50-100M\$) e soltanto l'8% investe più di 100M\$. Queste cifre, secondo il 68% degli intervistati, sono destinate a rimanere invariate durante il 2010, complicando ulteriormente la sfida degli IT manager che saranno chiamati a sfruttare al meglio le risorse a disposizione inclusi hardware, software e personale tecnico.

### **Disaster recovery: i test migliorano ma restano sempre una grande sfida**

Quest'anno il 26% degli intervistati italiani ha riferito di eseguire i test DR con una frequenza semestrale, mentre il 22% con frequenza annuale. Inoltre, è emerso che un test su quattro si rivela fallimentare, evidenziando un forte bisogno di miglioramento in questo senso. Alcune delle ragioni più ricorrenti per le quali le aziende italiane omettono i test sono le seguenti:

- mancanza di risorse in termini di tempo del personale (44%)
- interruzione delle attività per i dipendenti (44%)
- problemi di budget (40%)
- disservizi ai clienti (34%)

Un altro aspetto preoccupante è dato dal fatto che, rispetto agli anni passati, un numero maggiore di aziende ritiene che l'impatto dei test di disaster recovery si ripercuota significativamente su clienti, fatturato e brand reputation. Il 48% degli intervistati italiani ha, infatti, ammesso che questo tipo di test peserebbe sulla propria clientela e sulla brand reputation, il 46% che impatterebbe su vendite e utili, il 42% sulla perdita dei dati e sulla competitività. Symantec propone alle imprese una serie di metodologie di test DR da eseguire frequentemente e senza alcuna interruzione sulle operazioni aziendali. Symantec ritiene, infatti, che le persone e i processi rappresentino la ragione principale del fallimento dei test, mettendo così in evidenza la maggiore necessità di automazione in questo campo.

### **La virtualizzazione continua a essere una grande sfida**

Il 62% degli intervistati italiani ha affermato che la virtualizzazione è la ragione che porta a rivedere i piani di disaster recovery, mentre la metà dei server virtuali utilizzati in azienda risulta essere coperta da un piano di DR.

Il 46% degli intervistati ha additato la differenza degli strumenti per gli ambienti fisici e virtuali come le sfide maggiori alla protezione dei dati negli ambienti virtuali, mentre il 40% ha segnalato la mancanza di capacità storage per il backup e di strumenti avanzati di recovery.

A livello mondiale la ricerca ha rivelato per la metà degli intervistati alcuni altri importanti elementi:

- La mancanza di strumenti per la gestione storage costituisce la sfida primaria nella protezione dei dati e delle applicazioni mission-critical all'interno degli ambienti virtuali (53%)
- Le limitazioni in termini di risorse, come personale, budget e spazio, rappresentano le maggiori sfide alle procedure di backup delle macchine virtuali, generando il bisogno di una maggiore automazione e di una migliore capacità nel fare leva sugli investimenti IT esistenti al fine di abbassare i costi (51%)

### **Indicazioni**

Come questo studio ha dimostrato nel corso degli anni, la mancanza di risorse continua a rappresentare un problema, nonostante i costi del downtime siano sbalorditivi. Le imprese possono agire in questo senso implementando soluzioni

di automazione che minimizzino l'azione umana e che risolvano anche altri punti deboli presenti nei piani di disaster recovery.

Dato che i test di disaster recovery sono inestimabili ma rappresentano pur sempre un rischio di impatto sostanziale sull'azienda, inclusi clienti e fatturato, le imprese dovrebbero ottimizzare il successo dei test prendendo in considerazione e implementando metodologie trasparenti nei confronti della loro operatività.

Per concludere, le imprese dovrebbero includere nei piani di disaster recovery i responsabili della virtualizzazione, soprattutto per quanto riguarda le iniziative di test e backup. Gli ambienti virtuali dovrebbero essere trattati come server fisici, e le aziende dovrebbero essere disposte ad adottare strumenti multi-piattaforma e multi-ambiente, o a standardizzarsi su un numero inferiore di piattaforme.

“Questa edizione dello studio identifica con chiarezza gli aspetti cruciali legati a questo tema, i relativi rischi nascosti e le best practice per l'implementazione di soluzioni DR. Se da un lato alcuni aspetti registrano una tendenza positiva, dall'altro l'impatto del downtime risulta più pesante che mai”, ha spiegato **Giancarlo Marengo, Country Manager Symantec Italia**. “Il costo crescente del downtime mette ancora più in risalto l'aspetto economico del problema, il che si traduce in una maggiore pressione sull'IT. Se le imprese non proteggono i loro ambienti virtuali, non eseguono i test dei loro piani DR e assistono al fallimento di un test su quattro, allora è necessario introdurre tempestivamente un cambiamento verso una migliore gestione del rischio. Le aziende dovrebbero pertanto implementare soluzioni in grado di risolvere tali necessità, consentendo allo stesso tempo di fare leva sulle risorse esistenti”.

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

Giunto alla sua quinta edizione, lo studio Symantec Disaster Recovery Research 2009 è un'analisi annuale globale che Symantec commissiona con l'intento di fotografare le tendenze delle aziende in materia di preparazione e pianificazione nel disaster recovery. Condotta dalla società di ricerche indipendente Applied Research durante il mese di giugno 2009, lo studio ha coinvolto oltre 1.650 IT manager di grandi aziende in 24 Paesi fra Stati Uniti, Canada, Europa, Medio Oriente, Asia Pacifico e Sudamerica, con l'obiettivo di comprendere e analizzare alcuni degli aspetti più complessi associati al disaster recovery.

### **Informazioni su Symantec**

Symantec è il leader globale nella creazione di soluzioni per la sicurezza, lo storage e la gestione dei sistemi in grado di aiutare aziende e consumatori a proteggere e gestire le informazioni. I nostri software e servizi proteggono da un numero maggiore di rischi e in diverse situazioni, in modo più completo ed efficiente, per una maggiore fiducia dell'utente ovunque siano usati o archiviati dati.

Per ulteriori informazioni, consultare il sito web all'indirizzo [www.symantec.com](http://www.symantec.com) o [www.symantec.it](http://www.symantec.it)

###

**NOTE PER GLI EDITORI:** Per maggiori informazioni riguardo Symantec Corporation e i suoi prodotti è possibile visitare la Symantec News Room all'indirizzo <http://www.symantec.com/news>.

Symantec e il logo Symantec sono marchi o marchi registrati di Symantec Corporation o di sue consociate negli Stati Uniti e in altri Paesi. Gli altri nomi citati possono essere marchi appartenenti ai rispettivi proprietari.