September 11, 2007

Six Years After 9/11, Most Firms Are Not Ready For Another Disaster

by Stephanie Balaouras
for IT Infrastructure & Operations Professionals

FORRESTER® Making Leaders Successful Every Day

Includes data from Business Data Services

September 11, 2007

Six Years After 9/11, Most Firms Are Not Ready For Another Disaster

by Stephanie Balaouras
with Christine E. Atwood, Galen Schreck, and Rachel A. Dines

EXECUTIVE SUMMARY

Despite such devastating disasters and disruptions as 9/11, the European floods of 2005, and Hurricane Katrina, there is still significant room for improvement when it comes to enterprise disaster recovery preparedness. According to Forrester's Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007, approximately 27% of enterprises do not have a recovery site in the event of data center site failure; 23% of enterprises never test their disaster recovery plans, and 40% test their plans once per year. These results show that some enterprises still struggle to create convincing business cases for disaster recovery investment while others struggle with the ability to schedule business and application downtime to conduct adequate disaster recovery testing. All told, it's likely that IT operations professionals are crossing their fingers and hoping a disaster won't hit, while business executives have no idea how vulnerable they really are to significant losses — or to going out of business altogether.

TABLE OF CONTENTS

NOTES & RESOURCES

From April through June 2007, Forrester surveyed 189 data center decision-makers at North American and European enterprises about their disaster recovery preparedness, including whether or not they had a failover site, the maximum distance between their data centers, and how often they test their plans.

Research Documents

"Blue Cross: A Case Study In Building Better Disaster Recovery — While Saving Money" February 13, 2007

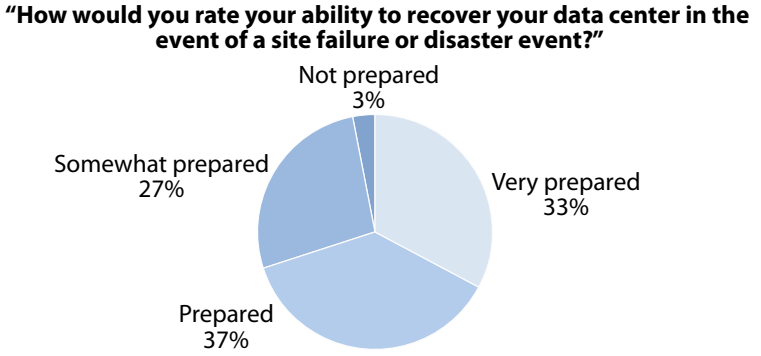
"Workforce Continuity Is A Critical Strategy In Your Business Continuity Plan" December 27, 2006

"Enterprises Are Realistic About Site Separation" June 5, 2006

ENTERPRISE DISASTER RECOVERY PREPAREDNESS IS LIKE A BOX OF CHOCOLATES

In early 2007, we surveyed 189 data center decision-makers at North American and European enterprises about their disaster recovery (DR) preparedness.[1] We found that while nearly two-thirds did have at least one backup data center or some kind of recovery site to act as a failover for their production data center, nearly 50% located their recovery site less than 50 miles (or 80 kilometers) away, and nearly a quarter never tested their DR plan. This begs the question, how prepared are enterprises for a disaster? Nearly 70% of respondents consider themselves prepared or very prepared — but is that really the case (see Figure 1)?

Figure 1 Enterprises Believe They're Ready For A Disaster



Base: 124 data center decision-makers at North American and European enterprises with a backup data center

Source: Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007

42946 Source: Forrester Research, Inc.

Disaster Recovery Presupposes You Have A Recovery Site

Enterprises typically have a set of conditions that must be met before a disaster is declared. Every attempt is made to continue or salvage operations at the primary data center, and only after a certain threshold is reached does the designated disaster recovery team leader activate the plan. There are some site disruptions that only disable the site for a few hours or days (i.e., a loss of water or a loss of power), and then it's easy to move back into the facility. However, there are disasters or disruptions that can disable the site for an extended period of time, and then it's necessary to have a recovery site. Without a designated recovery site, your recovery time capability will be weeks, potentially even months — if you recover at all — because it will take too long to secure a suitable site. According to our survey respondents:

- **More than a quarter of surveyed enterprises do not have a backup data center.** Of the 189 enterprises we surveyed, nearly 50% had one backup data center or recovery site, and an additional 16% reported having more than one (see Figure 2). While this is a promising result, it still leaves more than a quarter of these enterprises without a backup data center. However, 10% of those companies are planning for a second location within the next 12 months. If you currently do not have a backup data center, within 12 months you will be part of a very small minority.

- **A growing number of organizations are exploring "disaster recovery cooperatives."** In a cooperative, a group of organizations pool their financial resources to construct a shared facility, lease floor space from a collocation provider, or use one another's data center as a recovery site for the other. This is an emerging trend; most of the organizations that are using some kind of cooperative model have been state or local governments. It may be more difficult for private companies to pursue because of the legal agreements that would need to be hashed out to protect each company from significant liability.

Enterprises Are Taking DR Back "In-House"

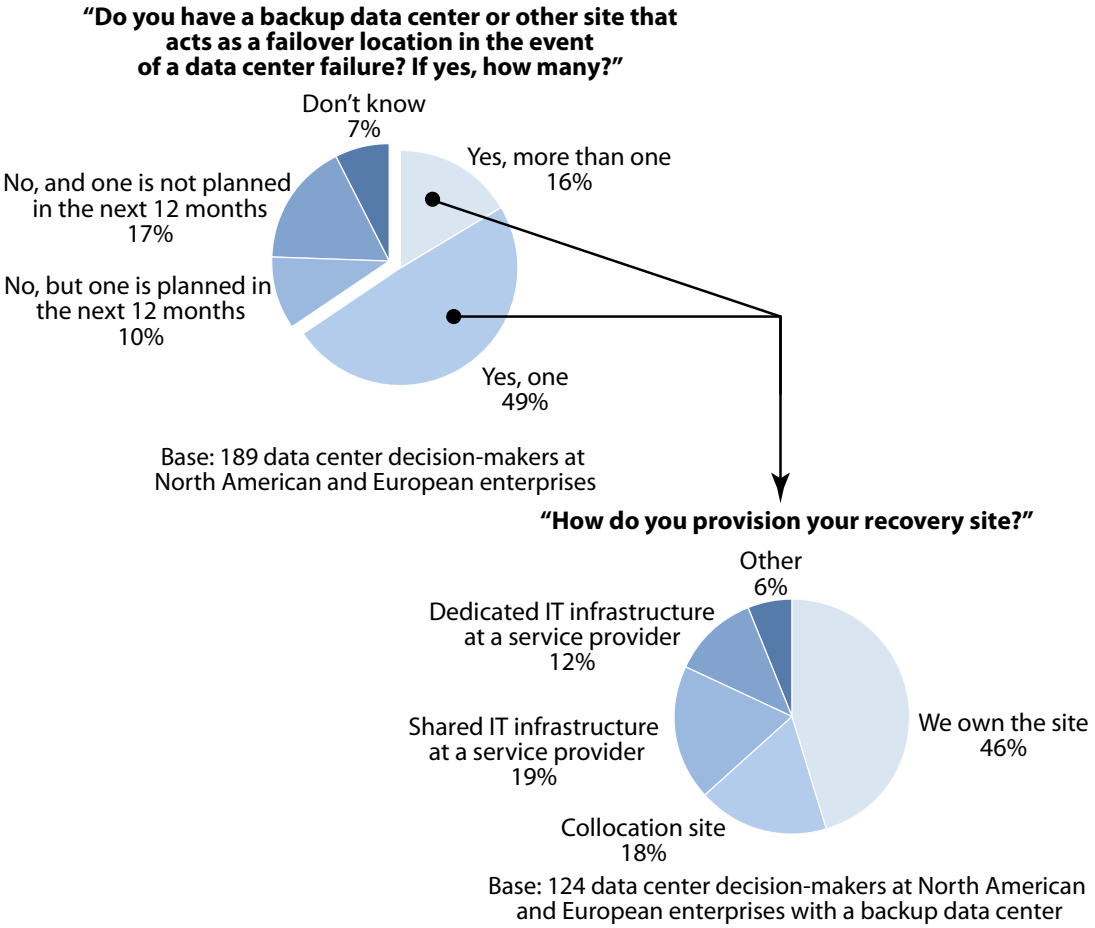
Of the 65% of enterprises we surveyed that do have at least one backup data center or recovery site, 64% say they run it themselves using an internal site or leased space from a collocation provider. Only 31% of these enterprises say they use traditional fixed-site recovery services from a DR provider. These survey results validate a trend that Forrester has seen with clients individually. There are several drivers behind the trend away from shared services:

- **Controlling recovery time.** Highly demanding recovery time and recovery point objectives can't be met with traditional shared-site fixed-recovery services. Typically, the shared IT infrastructure model cannot support recovery time objectives of less than 24 hours. According to our survey, only 19% of respondents use a shared IT infrastructure.

- **Signing lengthy and inflexible contracts with DR service providers.** Forrester clients often complain about inadequate testing blocks and the inability to schedule tests at mutually acceptable times. Companies must also be careful to ensure that their contracts provide enough flexibility to accommodate changing disaster recovery requirements due to mergers, acquisitions, divestitures, etc.

- **Putting existing assets to work.** Larger enterprises typically have more than one data center, so it's a matter of taking advantage of the two data centers to create a disaster recovery configuration between the sites. In addition, more and more enterprises are deploying technologies such as server virtualization and storage area networks at multiple data centers, and creating their own DR configurations using array-, network-, and host-based replication. Server virtualization increases flexibility in resource "repurposing" between DR and other deferrable workloads (i.e., application development, test, QA, etc.) at the backup data center.

Figure 2 A Majority Of Enterprises Now Have A Backup Data Center



Source: Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007

42946 Source: Forrester Research, Inc.

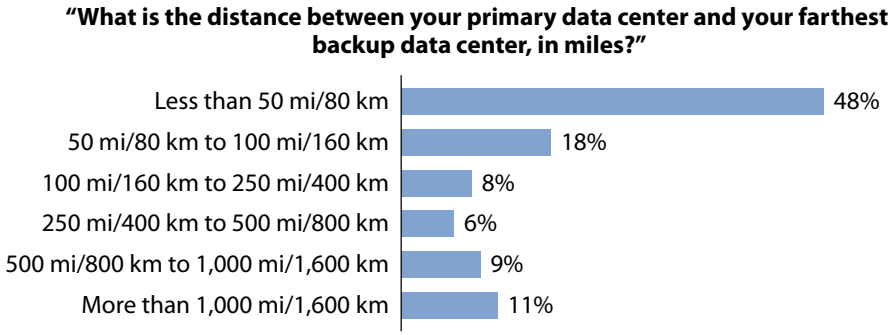
Enterprises Favor A Shorter Distance To The Recovery Site

There is no "rule of thumb" when it comes to the appropriate distance between your data center and your recovery site. You have to achieve enough distance between sites to escape the same set of threat events while balancing recovery requirements, technology limitations, and cost. Excessive site separation can affect application performance, recovery time, staff, and costs. However, if sites are subject to the same set of risks and threats, you don't have a disaster recovery configuration, you just have a very expensive high-availability configuration. To determine the appropriate distance, you must conduct a local threat assessment.

Enterprises leave themselves open to risk by keeping their backup data center too close to home. Of the 124 North American and European enterprises that currently have a backup data center, an astounding 48% have a distance of less than 50 miles (80 kilometers) between their primary data

center and farthest failover site (see Figure 3). In fact, only 33% have their farthest backup located more than 100 miles (160 kilometers) away from their primary location.

Figure 3 Many Enterprises Locate Their Backup Data Centers Close To Home



Base: 124 data center decision-makers at North American and European enterprises with a backup data center
Source: Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007
42946 Source: Forrester Research, Inc.

To Test Or Not To Test, That Is The Question

While a good first step toward disaster preparedness is to create, document, and disseminate a plan — how will you know its effectiveness if it goes untested? When asked how enterprises would rate their ability to recover their data center in the event of a site failure or disaster event, 33% of respondents considered themselves very prepared. In fact, only 3% reported they felt unprepared for a disaster, despite the fact that nearly a quarter of enterprises never test their plan, and 40% test their plans only once per year (see Figure 4). Forrester believes that most enterprises have a false sense of security when it comes to disaster recovery preparedness:

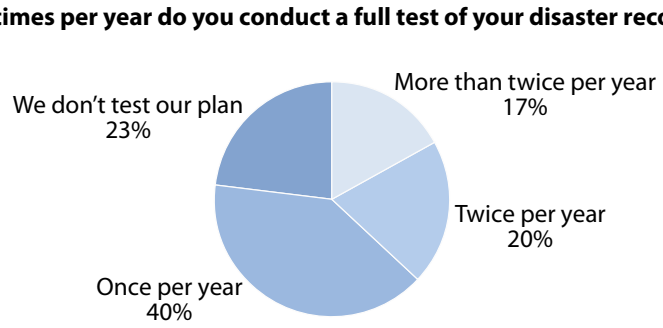
- **Complex plans need practice to become second nature.** Without regular testing of the disaster recovery plans, there's only a slim chance that an enterprise, particularly under the strain and duress of an actual disaster, could actually recover its mission-critical applications in the proper sequence at a recovery site.

- **Half a test isn't a realistic measure of preparedness.** Forrester often finds that enterprises that do claim to test their DR plans regularly actually conduct less thorough tests, such as testing an individual application rather than a full-scale data center disaster recovery test or a test of a group of dependent applications for process-centric recoveries.

Only 37% of enterprises reported testing their plans twice per year or more. Forrester believes that enterprises should strive to conduct a full-scale test at least twice per year, punctuated by process-centric recoveries as needed, particularly anytime there is a major configuration change. Testing is the best way to validate your recovery point and recovery time capabilities, validate configurations between the data center and recovery site, and train staff.

Testing is a challenge; it's risky and complicated to attempt a full-scale data center failover, and it's just as risky and complex to fail back. As a result, some enterprises opt to conduct their disaster recover tests using data copies at the recovery site. This type of test assumes that you electronically replicate data between sites and that you have the ability to create and split off a clone or a copy of the data. The recovery, restart, and consistency check of file systems, databases, and applications is performed with copies of production data. Some enterprises actually do perform a full data center failover and opt to run for a period of time at the recovery site before failing back — this is referred to as a planned workload rotation. Planned workload rotations are very effective at validating disaster recovery preparedness and training the IT organization.

Figure 4 There's Still Room For Improvement When It Comes To DR Testing



Base: 124 data center decision-makers at North American and European enterprises with a backup data center
Source: Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007

42946 Source: Forrester Research, Inc.

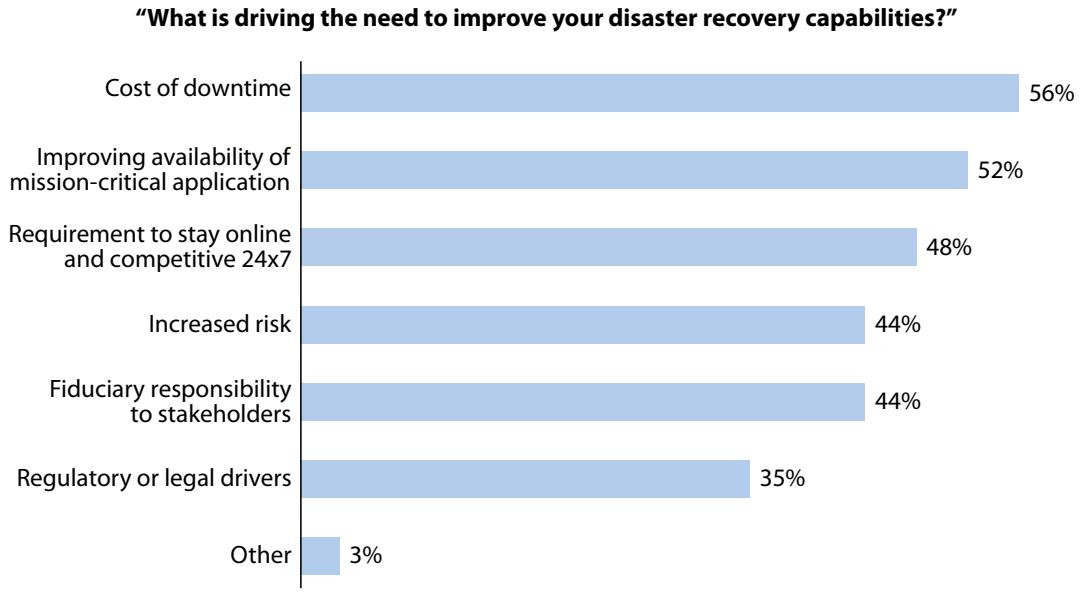
COST OF DOWNTIME IS STILL THE DRIVING FORCE OF DR PREPAREDNESS

Enterprises cited a wide range of reasons driving the need to improve their disaster recovery capabilities. Topping the list, with more than half of the respondents, were cost of downtime and the desire to improve the availability of mission-critical applications (see Figure 5). Not far behind was the requirement to stay online and competitive 24x7 (with 48% of respondents) and increased risk and fiduciary responsibility to stakeholders (both with 44% of respondents). Regulatory or legal requirements were lowest on the list. While regulatory or legal issues are often cited as important drivers of DR preparedness, in reality, regulations such as Sarbanes-Oxley (SOX), which applies to all publicly traded companies in the US, are very vague when it comes to DR specifics. SOX requires companies to preserve the integrity of their financial accounting and reporting systems regardless of the state of the enterprise. Proof of business continuity and disaster recovery readiness has become part of SOX compliance, but there is no standard by which to measure "readiness."

It's About Business Resilience, Not Just Insurance

The survey results indicate that enterprises are beginning to regard disaster recovery not just as an insurance policy in the event of major disaster but as an ongoing strategy that's vital to business operations and competitiveness. The highest-ranked drivers of DR preparedness — limiting cost of downtime, improving the availability of mission-critical applications, and staying competitive — indicate that some enterprises are determined to maintain their revenue, customers, and market share regardless of the disaster or disruption that comes their way. Disaster recovery implies that the organization has taken a hit that completely or severely incapacitated it, and the company needs to *recover* from a beaten down state. Resilience is defined as "the property of a material that enables it to resume its original shape or position after being bent, stretched, or compressed; elasticity."[2] A *resilient* business therefore might take a hit of some sort, but it's never severely incapacitated.

Figure 5 Cost Of Downtime Drives Improved DR Preparedness



Base: 124 data center decision-makers at North American and European enterprises with a backup data center (multiple responses accepted)

Source: Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007

42946 Source: Forrester Research, Inc.

RECOMMENDATIONS

EMBED RESILIENCE IN THE COMPANY CULTURE

- **Involve business owners in disaster recovery planning and budgeting.** Business owners must really be committed to DR if a company is going to move toward resiliency. Line-of-business owners (LOBs) or application owners must work with IT infrastructure and operations professionals to perform a business impact analysis (BIA) and threat assessment. LOBs should define recovery time and recovery point objectives based on the potential impact to the business (i.e., lost revenue, fees, etc.). Without the BIA, it's difficult to get the appropriate DR funding.
- **Create the business case for DR investments based on the impact to the business.** The more you can quantify the cost of downtime, the more likely you are to secure the appropriate funding for "resilience" efforts. In an ideal world, the company performs the BIA and then a local threat assessment, and IT gets the appropriate funding for infrastructure and technology. But obviously this is not always the case; the chances that you have a BIA that's current or that will be done before your next IT budget is due are low. You may have to work with LOBs and application owners to approximate the impact and create the best business case possible.
- **Institute centralized DR governance.** This is about getting your house in order. If your DR plans haven't been updated in three years, and you lack formal plans for every business unit, department, or entity using a different plan template, then start here. Use a common DR template that sets the minimum standard for a comprehensive DR plan and store all plans in a centrally accessible location. Set the required testing frequency and reporting requirements and audit DR plans on a regular basis to ensure compliance with the corporate standard. This is one low-cost way to improve preparedness and resiliency.
- **Make reasonable investments in technology and recovery site alternatives.** Not every company needs to have more than one backup data center and use high-end storage replication technology for zero data loss and downtime. But if you don't have an alternate site and you're still backing up to tape, it's time to re-evaluate your strategy.
- **Test plans often.** This point can't be reiterated enough. Frequent testing of plans is the only means by which you can reasonably assess your preparedness — unless you've actually declared a disaster in the recent past and successfully recovered from it. Full-scale tests should ideally be performed biannually, but annually is the absolute minimum. Whenever possible, schedule process-centric recoveries to test the ability to recover a critical business operation and its dependent applications. Process-centric recoveries are more important than individual application recoveries.

ENDNOTES

[1] Source: Enterprise And SMB Hardware Survey, North America and Europe, Q3 2007.

[2] Source: *The American Heritage Dictionary of the English Language*, Fourth Edition, Houghton Mifflin.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia
Brazil
Canada
Denmark
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Switzerland
United Kingdom
United States

For a complete list of worldwide locations, visit www.forrester.com/about.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®

42946