THE STATE OF BC/DR PREPAREDNESS

By STEPHANIE BALAOURAS
Due to increased competition, increased risk, and increased oversight and fiduciary responsibility, business continuity (BC) and disaster recovery (DR) preparedness is a critical priority at large and small companies alike. But getting started is difficult, and building the business case to obtain adequate funding is even more difficult — especially when companies are at various phases of BC and DR maturity. Forrester Research and the Disaster Recovery Journal have partnered to field a number of market studies in business continuity and disaster recovery in order to gather data for company comparison and benchmarking and to guide research and publication of best practices and recommendations for the industry. This is the first study, and it’s focused on gathering a baseline of company DR preparedness. Specifically, this study was designed to determine:

- How much companies are spending on DR.
- Company practices regarding DR planning, DR plan maintenance, and DR testing.
- The percentages of companies that have alternate recovery sites, the number of sites, and the distance between sites.
- Current recovery objectives and technology selection.
- Company confidence in DR preparations and preparedness.
- The most common causes of disaster declarations and downtime and the cost of downtime.
- Market drivers fueling continued improvement in DR preparedness.

**Study Methodology**

In October 2007, Forrester Research and the Disaster Recovery Journal (DRJ) conducted an online survey of 250 DRJ members. In this survey:

- 33 percent of respondents were from companies that had 0 to 999 employees; 25 percent had 1,000 to 4,999 employees; 20 percent had 5,000 to 19,999 employees; and 22 percent had 20,000 or more employees.
- 36 percent of respondents were from companies with revenues of less than $500 million; 10 percent were from companies with revenues of $500 million to $999 million; 19 percent were from companies with revenues of $1 billion to $4.99 billion; 8 percent were from companies with revenues of $5 billion to $10 billion; and 15 percent were from companies with revenues of more than $10 billion.
- All respondents were decision-makers or influencers in regards to planning and purchasing technology and services related to disaster recovery.
- Respondents were from a variety of industries.

**Figure 1 DR Spending**

<table>
<thead>
<tr>
<th>Annual disaster recovery spend by annual revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>$20 million and greater</td>
</tr>
<tr>
<td>&gt;$10 billion</td>
</tr>
<tr>
<td>11%</td>
</tr>
</tbody>
</table>

Base: 250 disaster recovery decision-makers and influencers at businesses globally

(Percentages may not total 100 because of rounding)


Source: Forrester Research, Inc.
This survey used a self-selected group of respondents (DRJ members) and is therefore not random. These respondents are more sophisticated than the average. They read and participate in business continuity (BC) and disaster recovery (DR) publications, online discussions, etc. They have above-average knowledge of best practices and technology in BC/DR. While nonrandom, the survey is still a valuable tool in understanding where advanced users are today and where the industry is headed.

**Disaster Recovery Spending Increases With Company Revenue**

Overall, DR spending is low, according to our survey; 45 percent of respondents spend less than $500,000 annually on disaster recovery, and 20 percent spend between $500,000 and $1.49 million. Spending increases with company revenue, which isn’t surprising; the higher the company revenue, the more the company is willing to spend to protect revenue from probable causes of operational downtime (see Figure 1).

**Disaster Recovery Planning, Maintenance, And Testing Is Improving**

Perhaps one of the biggest challenges to effective DR preparedness is planning, maintenance, and testing. Through client inquiries and advisories, Forrester finds that many companies don’t have formal plans in place, and if they do have plans, they aren’t integrated into regular configuration management and change management processes, and they are not regularly tested. According to Forrester’s Enterprise and SMB Hardware Survey, North America and Europe, Q3 2007, approximately 23 percent of enterprises (companies with more than 1,000 employees) never test their disaster recovery plans. By contrast, Forrester found in this survey that:

- **A majority of companies has formal DR plans in place.** Approximately 79 percent of respondents already have formal DR plans in place, and another 19 percent plan to have formal DR plans in place in the next year.
- **Almost one-third of companies continuously update plans.** The best practice in plan maintenance is to ensure that DR plans are continuously updated as part of configuration management and change management. Another 14 percent of respondents update their plans at least quarterly.

---

**Figure 2 DR Planning, Maintenance, And Testing**

2-1. "Do you have a formal and documented disaster recovery plan in place?"

- No, we currently do not have plans to develop a formal business continuity plan (2%)
- No, but one is currently planned in the next 6-12 months (19%)
- Yes (79%)

Base: 250 disaster recovery decision-makers and influencers at businesses globally

2-2. "How often is your disaster recovery plan updated?"

- Continuously (our DRP is updated as part of change and configuration management process) (26%)
- Quarterly (14%)
- Twice per year (18%)
- Every two years (3%)
- I can’t remember the last time we updated our DRP (7%)
- Don’t know (3%)

Base: 250 disaster recovery decision-makers and influencers at businesses globally

2-3. "How many times per year do you conduct a full test of your disaster recovery plan?"

- More than twice a year (10%)
- Twice a year (22%)
- Once a year (34%)
- We don’t test our plan (14%)
- Don’t know (4%)

(Percentages may not total 100 because of rounding)

Base: 250 disaster recovery decision-makers and influencers at businesses globally

Source: Forrester Research, Inc.

---

**Figure 3 Disaster Recovery Sites**

3-1. "How do you provision your recovery site?"

- We own the site (34%)
- Shared IT infrastructure at a service provider (30%)
- Dedicated IT infrastructure at a service provider (12%)
- Colocation site (11%)
- Other (9%)
- Don’t know (3%)

Base: 250 disaster recovery decision-makers and influencers at businesses globally

3-2. "What is the distance between your primary data center and your farthest backup data center?"

- Less than 25 miles (21%)
- 25 miles to less than 50 miles (14%)
- 50 miles to less than 100 miles (9%)
- 100 miles to less than 250 miles (6%)
- 250 miles to less than 500 miles (13%)
- 500 miles to less than 1,000 miles (13%)
- 1,000 miles and greater (19%)
- Don’t know (5%)

(Percentages may not total 100 because of rounding)

Base: 250 disaster recovery decision-makers and influencers at businesses globally

Source: Forrester Research, Inc.
One-third of companies test their plans at least twice a year. Forrester recommends that companies conduct at least two full tests per year, followed by several component tests throughout the year. Fifty percent of companies still only test once a year, and 14 percent never test (see Figure 2).

Companies Prefer Dedicated IT Recovery Infrastructure, And Site Separation Is Increasing

Companies clearly prefer dedicated infrastructure. According to our survey, 57 percent of respondents use dedicated IT infrastructure, whether that’s at an internal site (34 percent), collocation site (11 percent), or service provider site (12 percent). With dedicated infrastructure, companies can achieve a much better time to recovery and improve their recovery point with the use of replication (see Figure 3-1).

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. We found that DRJ members favor greater distances than the enterprise decision-makers we surveyed. According to Forrester’s Enterprise And SMB Hardware Survey, North America And Europe, Q3 2007, approximately 48 percent of enterprises have sites less than 50 miles apart. By contrast, Forrester found that only 35 percent of DRJ members have sites less than 50 miles apart (see Figure 3-2).

More And More Applications Are Considered Critical

When asked to classify what percentage of applications fell into mission-critical, business-critical, and non-critical categories, it appears that companies are less likely to classify applications as non-critical. On average, respondents classified approximately 35 percent of applications as mission-critical, 37 percent as business-critical, and 28 percent as non-critical.

Tape is still the dominant recovery technology. For all applications and data sets, regardless of criticality, tape still remains an important part of disaster recovery preparedness. This means that while the use of replication is increasing, companies will still perform traditional backups as a precaution and to ensure that they have a history of recovery points.

Companies are expanding the use of replication. Replication is no longer used only for mission-critical applications. The survey
indicates that companies use synchronous and asynchronous replication to protect business-critical applications (see Figure 4).

Companies Now Measure Their Expected Recovery In Hours

With dedicated IT infrastructure at the recovery site and expanded use of replication, recovery time and recovery point objectives are now measured in hours. Sixty-five percent of respondents reported that they would lose less than 10 hours of mission-critical data and 46 percent reported that they could recover mission-critical applications in less than 10 hours (see Figure 5).

Most Declared Disasters And Disruptions Are Preventable

According to our survey, approximately 72 percent of companies have never officially “declared disaster” in the past five years. Companies should not take comfort in this statistic. It still means that almost 28 percent of companies are likely to “declare disaster” and failover to their alternate site in a five-year time period, and it doesn’t take into account the events that disrupt operations but don’t affect the entire data center. The survey also found that:

- The most common cause of declared disaster is power failures. Forty-two percent of respondents indicated that a power failure was the cause of their most significant disaster declaration or major business disruption, followed by IT hardware failures and network failures (see Figure 6).
- Most companies can recover operations in less than 10 hours after a declared disaster. Of the 190 respondents to our survey that have had to declare a disaster or suffered a major business disruption, 62 percent recovered operations in less than 10 hours.
- Most companies will lose less than 10 hours of data in a declared disaster. Of the 190 respondents to our survey that have had to declare a disaster or suffered a major business disruption, 83 percent lost less than 10 hours of data.
- 64 percent of companies don’t know the cost of their most recent declared disaster or disruption. So IT operations has improved planning, maintenance, testing, and actual response but still can’t actually measure the cost of a declared disaster. For the 12 percent of companies that do know their costs, the average total cost of a declared disaster is approximately $1.9 million.

DR Preparedness, Companies Still Strive For Improvement

Companies are confident about their current DR preparedness, and for those that have experienced disasters or disruptions, recovery capabilities are now measured in hours. With dedicated IT infrastructure at the recovery site and expanded use of replication, recovery time and recovery point objectives are now measured in hours. Sixty-five percent of respondents reported that they would lose less than 10 hours of mission-critical data and 46 percent reported that they could recover mission-critical applications in less than 10 hours (see Figure 5).
hours. But despite all these efforts, there is still a push to improve recovery capabilities even further (see Figure 7).

When respondents were asked to identify what was driving their need to improve disaster recovery preparedness, fiduciary responsibility was ranked the highest, followed by the need stay online and competitive, and the cost of downtime (see Figure 8). The survey results indicate that DR preparedness is gaining awareness and importance with constituents outside of IT; it's now a priority with strategic senior executives, stakeholder, partners, and customers.

Stephanie Balaouras is a senior analyst for Forrester Research. Balaouras primarily contributes to Forrester's offerings for IT infrastructure and operations professionals. She is a leading expert in how companies build resilient IT infrastructures to support key business initiatives. Balaouras has more than 10 years experience with technology for information storage, information protection, and disaster recovery. Balaouras holds a bachelor's degree in business administration and finance and investments from Babson College.

When Your Next Work Disruption Occurs

- Can your employees continue to work no matter where they are located?
- Does your emergency preparedness account for your entire workforce?
- Can you confirm your employees are safe and able to access critical business applications?

IBM Virtual Workplace Continuity, powered by Citrix, is a completely hosted solution that enables a disrupted workforce to easily switch to a virtual work environment—keeping productivity high during disruptions such as transit strikes, avian flu pandemic or hurricanes. Business continuity professionals can notify/alert their workforce of a disruption, account for employee safety, and easily share status updates to management throughout the disruption. From any remote location, employees can easily continue to access critical business applications when disruptions prevent them from getting to their work location, as well as communicate and collaborate with their peers, customers and partners.