The State Of Disaster Recovery Preparedness 2017

By STEPHANIE BALAOURAS
Forrester Research and the *Disaster Recovery Journal* have partnered to field a number of market studies in business continuity (BC) and disaster recovery (DR) 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 study, which focuses on DR preparedness, was first fielded in the fall of 2008 and then again in 2011 and 2013. We designed this year’s study specifically to determine:

**Figure 1 DR Preparedness**

“How would you rate your ability to recover your data center in the event of a site failure or disaster event?”

<table>
<thead>
<tr>
<th>Prepared 34%</th>
<th>Somewhat prepared 37%</th>
<th>Not prepared 17%</th>
<th>Very Prepared 18%</th>
</tr>
</thead>
</table>

A Slim Majority Feel Prepared For Major Disruption

Since we first fielded this study in 2008, we have seen dramatic increases in the adoption of advanced replication technologies and sophisticated multi-site data center architectures. Despite, these technological advancements, only 18 percent of respondents feel very prepared they could recover their data center in the event of a site failure or disaster event, and 37 percent rate themselves as prepared (see Figure 1). As we’ll see in the rest of the study, much of this lack of preparedness can be attributed to a lack of maturity in core planning processes, out of date plans, and very limited testing. It comes as no surprise then that the vast majority of organization say that improving DR at their firm

**Figure 2 Factors Driving DR Improvements**

“What is driving the need to improve your DR capabilities?”

| Requirement to stay online and competitive 24x7 | 43% |
| Regulatory or legal drivers | 39% |
| Cost of downtime | 39% |
| Increased risk (i.e. from natural disasters, man-made disasters etc.) | 30% |
| Improving the availability of a specific mission-critical application | 26% |
| Fiduciary responsibility to stakeholders, employees, partners, customers etc. | 24% |
| DR was identified as a top risk for the company | 24% |
| New systems/infrastructure that are critical to company success | 22% |
| Increased attention from leadership | 22% |
| Closer connection to corporate risk management function | 11% |

Base: 73 DR decision-makers
Source: Forrester/DRJ State Of DR Preparedness Survey 2017

Base: 54 DR decision-makers who said that it was critical to improve their company’s DR capabilities
Source: Forrester/DRJ State Of DR Preparedness Survey 2017
is a critical priority and while regulatory compliance continues to be a driver, it’s the business need to stay online and competitive 24x7 that’s the top driver (see Figure 2).

**DR Programs Report Into A Variety Of Leaders, And Not Always To A C-level Executive**

One item of good news, only 10 percent of respondents reported lacking any kind of formal DR program. The bad news? Only 54 percent reported having a unified program that spanned the entire enterprise (see Figure 3). For the remaining respondents, they have separate silos of DR planning or separate silos of DR planning loosely coupled by a DR program director or equivalent. Sometimes, particularly for large enterprises consisting of acquired companies or have business units that essentially act as independent businesses, the loosely coupled silo approach is the most feasible. However, for many years there has been a movement towards a stronger federated model where overall governance, strategy, policy, processes, and standards are set by a strong corporate group while local planners can customize specific plans for their region or business unit. Our study also revealed that:

► Many DR programs still report into the head of infrastructure and operations. According to our study, while 34 percent of DR programs report into the CIO and other 12 percent report into the CISO, a large percentage, 28 percent, report into infrastructure and operations (see Figure 4). Reporting into infrastructure and operations is not surprising given this where responsibilities for networking, storage, compute, and overall data center strategy and management reside, but it also creates challenges because it doesn’t always give the DR program director enough of an expansive view or the authority to ensure the resiliency of end-to-end IT services that support critical business functions.

**Figure 3 DR Program Formalization**

“Do you have a formal DR program in place today?”

- We have a formal DR program, with a director or similar who heads DR planning enterprise-wide
- We have several silos of DR planning but they are not connected by a single program
- We have several silos of DR planning guided by a single DR program director or head
- 3%
- 7%
- 15%
- 21%
- 54%

**Source:** Forrester/DRIU State Of DR Preparedness Survey 2017

**Figure 4 DR Program Reporting Structure**

“Into what function/role does the head of the DR program report?”

- CIO
- 31%
- CISO
- 11%
- Infrastructure and operations
- 25%
- Business continuity
- 8%
- Other
- 17%

**Source:** Forrester/DRIU State Of DR Preparedness Survey 2017

**Figure 5 DR Program Reporting Level**

“To which level within the organization does the head of disaster recovery directly report?”

- C-level or equivalent head of the functional area (e.g., COO)
- 45%
- Two levels below C-level or equivalent functional head
- 27%
- One level below C-level or equivalent functional head
- 18%
- More than two levels below C-level or equivalent functional head
- 11%

**Source:** Forrester/DRIU State Of DR Preparedness Survey 2017
The majority of DR program heads do not report to c-level executives. Only 45 percent of the heads of DR programs report directly into a c-level executive (see Figure 5). In fact, most are two to three levels removed from a c-level executive. This is a huge issue for organizations. If the DR program director doesn’t report directly into a c-level executive, he or she lacks not only the authority to enforce certain requirements but the influence to affect more significant change – such as influencing data center strategy, enterprise architecture, and application development and delivery.

Disaster Recovery Planning, Maintenance, And Testing Remain Areas For Improvements

Conducting a business impact analysis (BIAs) is critical to identifying critical business functions, mapping all IT dependencies and interdependencies, and defining recovery objectives. Conducting a risk assessment is critical to understanding what specific steps you can take to mitigate the most probable, high impact risks, and then developing plans for the residual risks that remain. Together, the BIA and risk assessment are the core inputs into your business case for DR investment, your risk mitigation strategies, architecture, and tech adoption, and your documented DR plans. Unfortunately, many organizations still fail to conduct and refresh these core planning functions with any sort of regularity (see Figure 6). Forrester recommends that organizations aspire to continuous BIAs and risk assessments rather than treating these processes as one-time or periodic updates.

Most experts will agree that running tests are the best way to ensure preparedness. In the past, survey results have returned disappointing results around organizations’ testing regimens. However, this iteration reveals some good news: 43 percent of organizations are now running a full test once – a slight increase from 39 percent in the prior study. However, only 19 percent (a decrease of 11 percent from the last study) run a full test twice per year or more frequently (see Figure 7). Additionally, with the rapid rate of business and IT change...
today, it’s critical that companies update their plans continuously, something that only 14 percent of organizations do today—a decrease from 35 percent in the prior study (see Figure 8).

Organizations Continue To Look To The Cloud And Colocation For DR Sites

DR in the cloud has been a hot topic that has garnered a significant amount of attention during the past few years. Adoption is increasing but at a slow rate. According to the latest survey, 18 percent of companies are now using the cloud in some way as a recovery site—an increase of 3 percent. This includes 10 percent who use a fully packaged DR-as-a-Service (DRaaS) offering and 8 percent who use Infrastructure-as-a-Service (IaaS) to configure their own DR in the cloud configuration. Use of colocation for recovery sites is remains consistent at 37 percent (roughly the same as the prior study). However, the most common method of sourcing recovery sites is still in-house at 43 percent (see Figure 9).

According to the latest survey, average distance between sites is approximately 354 miles, with a median of 74 miles. While there is no absolute right answer for how far apart recovery sites should be, the rule of thumb is that they should not be subject to the majority of the same risks. Our study also reveals that more organizations are moving to some kind of active-active data center configuration where both sites run production workloads in some manner or at least use it to run deferrable workloads (see Figure 10). Today, 46 percent describe their data center configuration as active-passive. Another iteration on the concept of active-active is the workload rotation strategy. In a workload rotation, organizations periodically failover/migrate production workloads to the alternate site (see Figure 11).
Firms Turn To Advanced Technologies To Protect The Growing Number Of Critical Systems

According to the 2015 Forrester/DRJ survey, the top risk that BC managers say they face today is the increased reliance on technology. Today, even in industries such as healthcare and manufacturing, there are fewer and fewer manual processes. This explains why 30 percent of systems are now considered mission critical and 34 percent are considered business critical – just 36 percent of systems now fall into the non-critical classification.

To address increasing business expectations and shrinking recovery time and recovery point objectives, more firms are turning to technologies such as replication not just for mission critical systems but also for business critical and even less critical systems. In fact, a surprising 53 percent say they use synchronous replication to protect mission critical systems – an increase of 4 percent from the prior study (see Figure 13). This is stunning given the amount of bandwidth required to support synchronous replication between sites. Legacy technologies like backup to tape still play an important role in DR plans but for the first time since we began running this study in 2008, it is effectively tied with snapshots as one of the most common methods for protecting non-critical systems. It’s worth noting that it is still in use with more critical systems, often as a tertiary protection method.

IT Failures Are The Top Culprits For ‘Disasters’

According to our study, 22 percent of organizations had to declare a “disaster” and failover operations to their recovery site at least once during the last five years. This doesn’t include organizations that likely had major disruptions of one or more systems but opted not to failover – a typical occurrence when many organizations lack confidence on their capabilities. The main culprits for declared disasters that require full failover are IT failures, including hardware, software, or network failures. The next two most common causes of declared disasters are power failures and floods, followed by cyberattacks, natural disasters and human error (see Figure 5).

We often most strongly associate “disaster” recovery with climactic events and or human-made disasters such as terrorist events and chemical spills but as the data shows study after study, it’s mundane events such as power failures, IT failures, and human error cause most downtime. DR planners should also...
take note of the impact of cyberattacks. Cyberattacks from ransomware attacks to DDoS attacks should not be treated as exclusively the domain of the security team. DR planning should account for any impact to the firm’s IT capabilities regardless of the source of the disruption or impact.

When we asked organizations that had declared a disaster to identify their biggest challenges or lessons learned from the event – mismatched business expectations with IT capabilities and insufficient testing and overall preparedness came out as the top two – proving once again that most DR preparedness deficiencies today can be traced back to a lack of maturing it governance and process.

Study Methodology

In the fall of 2016, Forrester Research and the Disaster Recovery Journal (DRJ) conducted an online survey of 90 DRJ members. In this survey:

▶ Thirty-nine percent of respondents were from companies that had 0 to 999 employees – what Forrester defines as small and medium businesses; 22 percent had 1,000 to 4,990 employees; 21 percent had 5,000 to 19,999 employees; and 16 percent had 20,000 or more employees.

▶ All respondents were decision-makers or influencers in regard to planning and purchasing technology and services related to disaster recovery.

▶ Respondents were from a variety of industries.

This survey used a self-selected group of respondents (predominantly DRJ members and Forrester clients) and is therefore not random. These respondents are more sophisticated than the average. They read and participate in business continuity and disaster recovery 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.

Stephanie Balaouras is a vice president, research director of security and risk for Forrester Research.