the Availability Digest

www.availabilitydigest.com

How Do Your Readiness Plans Stack Up?

January 2011

Unfortunately, Business-Continuity Planning (BCP) and Disaster Recovery (DR) are often at the bottom of the priority list when it comes to tight budgets. The premier publication for BCP, *The Disaster Recovery Journal*, usually has several articles trying to analyze why these activities are not of paramount interest to top management and how to approach top management to get their attention.

How are you doing in getting the support you need to build effective business-continuity and disaster-recovery plans? If you are one of those "top management" guys, are you doing your bit to ensure that your company will survive the ultimate disaster?

An interesting insight into these questions can be obtained by comparing the state of your readiness plans with those of your peers. Annual *Readiness* surveys by The Standish Group (www.standishgroup.com) provide this capability, and we report on their findings below. The Standish *Pinpoint* surveys study a number of enterprise questions. They represent the inputs of about 300 top managers from small, medium, and large companies. About 70% of these managers are with Fortune 500 companies. 20% represent mid-size companies, and the remaining 10% represent small companies.

Infrastructure

The Standish Readiness Survey contains several questions relating to readiness infrastructure. These surveys have taken place annually for several years, and the latest survey summarizes the results for the last four years. This gives an interesting indication as to the progress companies are making toward readiness.

With respect to a company's readiness infrastructure, the following results show the progress over the last four years. The percentage of positive results is shown for the years 2007 and 2010.

	2007	2010
Do you allocate high availability and software costs to your DR and BCP budget?	68%	85%
Do your systems monitor application processes for failure and automatically take corrective measures?	65%	88%
Do you have test suites developed to check that the critical failover functionality operates properly on newly configured systems?	42%	55%

	2007	2010
Do you have documented step-by-step procedures for recovering computing resources following a site catastrophe?	44%	76%

The first question is key – are you getting the budget you need in order to implement an effective readiness program? Can you obtain the critical hardware and software infrastructure components needed to maintain the required availability of applications and to recover them in the event of a disaster, or are these afterthoughts or workarounds? Most executives now feel that they are properly funded, up significantly from four years ago.

A critical part of the readiness infrastructure is the ability to monitor the data-center components and to detect failures. If a failure is detected, automatic action should be taken to immediately recover from the failure so that IT operations will not be affected. Today, it seems that most companies have invested in such facilities.

A major continuing weakness in disaster-recovery plans is failover testing. Just a little over half of the companies surveyed actively test their failover plans. Testing failover can be a very expensive and risky undertaking. However, the alternative to failover testing is *hope* – a blind faith that failover will work or can be made to work in a reasonable amount of time.

Interestingly, though only about half the companies do failover testing, three-quarters of them have prepared detailed documentation of failover procedures (the survey shows that 90% of companies either have documentation or plan to have it). This is extremely important since the middle of a failover crisis is not the time to be trying to figure out what to do. However, will an untested but well-documented plan work? We *hope* it will.

Unplanned Downtime

An important factor in high availability is the elimination of planned downtime. Planned downtime is often needed to upgrade hardware, system software, and networks. With proper facilities and procedures, upgrades can be made with no downtime required.

The typical technique for eliminating planned downtime is to upgrade a backup node and then to fail over to it and upgrade the primary node while the backup node is providing application services. Can the failover be done fast enough to qualify for no application outage? Will the failover work?

The survey measured the percent of infrastructure components that could be upgraded with no application outage. Though about half the companies could upgrade about half of their infrastructure without taking an application outage, almost none could totally avoid such outages. This is commensurate with the current use of active/active technology.

What percent of hardware, software, network, and other infrastructure components can be replaced or upgraded without requiring an application shutdown?	
Less than 33%	29%
33% to 65%	47%
65% to 99%	17%
100%	1%

For eliminating planned downtime, active/active technology[1] is the ultimate strategy. An active/active system is one in which multiple nodes, each with a replicated copy of the current

[1] What is Active/Active?, *Availability Digest*, October 2006.

application database, are actively processing the application workload. With these systems, failover simply involves sending the transactions normally being handled by the node to be upgraded to other surviving nodes in the application network. Failover can be accomplished in seconds, and it is known that the other nodes are currently operational.

Skills

The best infrastructure in the world is not much good if there is not a knowledgeable staff to operate and manage it. The Standish survey asks several questions concerning the skill levels in the organization. These questions and the responses follow. In the survey, the possible responses included “Highly,” “Skilled,” “Moderately,” and “Poorly/No.” The table below shows the percent that responded “Highly” or “Skilled.”

	2007	2010
Is your organization skilled in:		
maintaining critical hardware systems for readiness?	56%	73%
maintaining critical system software for readiness?	58%	71%
maintaining critical network operations?	49%	61%
maintaining critical computer operational environment (power, air conditioning, fire prevention, other)?	60%	74%
managing staff training and maintaining update procedures?	40%	50%
deploying application-level security monitors that detect when applications are using system resources in an inappropriate or unusual manner?	37%	55%
maintaining identical (synchronized) databases and files in both the primary and secondary sites?	28%	46%
maintaining hardware, software, network, and other infrastructure components so they can be replaced and/or upgraded without requiring an application shutdown?	49%	56%
creating application software for readiness?	46%	53%
maintaining critical business operations with duplicate peer-level people at more than one operational site?	32%	44%

Maintenance skill levels are relatively high (60% to 75%) – maintaining hardware, system software, networks, and environmental systems. The Standish Group points out that hardware maintenance is being performed more and more by company staff rather than through vendor support as equipment maintenance is simplified. Standish has seen a marked reduction in the number of service contracts with two-hour or less response times.

Coming in a poor second, hovering around 50%, are staff training, security, replication, and eliminating planned downtime. The low score for replication is disturbing since the maintenance of a reliable database copy is fundamental to high availability and disaster recovery. Developing recoverable applications was also low on the totem pole.

Of particular concern is that less than half the companies surveyed extended redundancy to people – having more than one person skilled in each task. Should a disaster happen, it is quite likely that one or more critical people will be unavailable (hopefully on vacation and not under a pile of rubble).

However, all in all, there has been significant improvement in all classes of skills over the four years covered by the surveys.

What's Important?

After all is said and done, a critical question is what is most important in achieving a reasonable state of readiness. Interestingly, those surveyed put technical expertise at the top by a large margin. A distant second and third were project management and vendor support – both are further forms of expertise.

What activities have a major impact on your high availability and readiness success?	
Technical expertise	78%
Project management	44%
Vendor support	35%
Executive sponsor participation	21%
User participation	14%

Having an effective executive sponsor was not rated very highly. This is surprising given the importance of a sufficient budget. However, since 85% of the respondents indicated that they were able to include readiness infrastructure in their plans, this may be understandable.

At the very bottom, with a mere 14%, is user participation. This is probably a reflection of the fact that users are important to application effectiveness but not so much to the underlying infrastructure.

Summary

The Standish Group Pinpoint surveys contain a great deal more detailed information than what is reported here. Standish subscribers can reference these Pinpoints by logging on, clicking on *Data Pinpoints*, and then selecting *Readiness*.

As the surveys show, the IT state of readiness is certainly improving as time passes and as application services become more critical to the survivability of the enterprise. However, in many cases, half of the surveyed companies still have a ways to go in many critical areas. They include failover testing, staff training, and staffing redundancy.

This adds impetus to the creation and maintenance of a good Business Continuity Plan. If all else fails and if IT is down, how is the business going to continue to function and survive?

The Standish Group

The Standish Group provides research services focused on improving project success through its CHAOS services and on enhancing the value of IT investments via its TCO/ROI benchmarks.