the Availability Digest

Aberdeen's 2008 Business Continuity Survey

April 2008

The Aberdeen Group, a major industry analysis firm, has published its most recent survey concerning the state of business continuity planning and implementation among a broad spectrum of small to large companies. This March, 2008, report, entitled Business Continuity: Implementing Disaster Recovery Strategies and Technologies, is publicly available at http://www.aberdeen.com/summary/report/benchmark/4662-RA-business-continuity-disaster-recovery.asp.

Aberdeen notes that 62% of the companies surveyed experienced between one and five business interruption events in the last year. 34% of all companies surveyed have yet to implement a solution. It seems that there remains a disconnect between reality and action in the marketplace when it comes to protecting a company's IT assets from failures and disasters.

The Survey Base

The survey focused on those enterprises that have implemented a business continuity/disaster recovery (BC/DR) solution. In all, 150 companies took part in the survey. The companies covered a worldwide range of small to large companies in a variety of industries:

- *Company size*
  - 28% of respondents were from large companies with revenues in excess of $1 billion.
  - 43% were from midsize companies with revenues between $50 million and $1 billion.
  - 29% were from small companies with revenues under $50 million dollars.

- *Geography*
  - 62% of respondents were from North America.
  - 17% were from EMEA (Europe, Middle East, and Africa).
  - 16% were from the Asia/Pacific region.

- *Industry*
  - 17% of respondents were in high technology industries.
  - 13% were in the financial industry.
  - 7% were in the public sector.
  - 6% were in the insurance and legal services industries.
  - The remaining 57% were spread across a broad range of other industries.

The survey questions were designed to determine the following:

- The degree to which the company is actively using a BC/DR system or is in the process of implementing such a strategy.

- The metrics used by the company to assess their progress in building and using a BC/DR system.

- The benefits that have been derived from implementing a BC/DR system.

Ranking of Organizations

Aberdeen used three key performance metrics to distinguish the quality of an organization's BC/DR efforts:

1. The ability to meet its Recovery Time Objective (RTO).
2. The time that it took to recover from its most recent business disruption.
3. The decrease in unplanned downtime that it had achieved.[1]

Based on these metrics, Aberdeen ranked the responding organizations into three tiers – Best in Class, Industry Average, and Laggard. The top 20% of organizations made the Best-in-Class tier. The bottom 30% were rated as Laggards. The middle 50% formed the Industry-Average tier.

The Performance of the Tiers

The results as measured by the three metrics above for each of the tiers are as follows:

Best in Class

1. 50% of organizations met their RTO 100% of the time. On the average, this tier met its RTO 93% of the time.
2. 95% recovered from the most recent disruption in less than one hour. The average recovery time was thirty minutes.
3. 41% achieved more than a 10% decrease in unplanned downtime. The average decrease was 8.7%.

Industry Average

1. 17% of organizations met their RTO 100% of the time. On the average, this tier met its RTO 83% of the time.
2. 19% recovered from the most recent disruption in less than one hour. The average recovery time was 2.1 hours.
3. 26% achieved more than a 10% decrease in unplanned downtime. The average decrease was 3.3%.

Laggards

1. 0% of organizations met their RTO 100% of the time. On the average, this tier met its RTO 70% of the time.
2. 0% recovered from the most recent disruption in less than one hour. The average recovery time was 15.7 hours.
3. 13% achieved more than a 10% decrease in unplanned downtime. The average decrease was 0.5%.

Continuity Plan Strategies

The creation and maintenance of a BC/DR plan is the underpinning for a successful BC/DR strategy. This plan must be continually updated, and it must be made readily available to those

[1] The survey results are silent upon what history this depended.

employees who are responsible for the execution of the plan. Above all, the plan should be tested regularly. BC/DR testing is an expensive and risky activity; but if the plan is not regularly tested, it may not work when needed.

The compliance of the three tiers of organizations with respect to these requirements is presented below.

	Best in Class	Industry Average	Laggards
Periodically Update Plan	84%	29%	23%
Make Plan Available to Employees	68%	52%	48%
Test Plan Regularly	53%	41`%	36%

Competitive Assessment

In addition to the key metrics used to determine in which tier an organization belonged, Aberdeen rated the companies on several other criteria. These criteria included:

- *Process* – Disaster recovery plan testing
- *Organization* – Cross-functional disaster recovery team
- *Knowledge* – a) Classify data based on business importance and retrieval need
  b) Visibility into mission-critical systems and data
- *Technology* – Storage area network[2]
- *Performance* – Percentage of data availability SLAs met over the past year

The scores that Aberdeen gave to each of the tiers for these criteria follow:

	Best in Class	Industry Average	Laggards
Plan Testing	79%	63%	42%
Recovery Team	74%	52%	37%
Data Classification	58%	50%	21%
Visibility	84%	56%	21%
SAN	63%	59%	47%
Data Availability SLA	100%	65%	50%

As mentioned earlier, BC/DR plan testing is one of the most important but often neglected actions that should be taken. Testing disaster recovery requires failing the primary system and failing over to the backup system. Such testing often requires weeks of planning, the assembly at test time of all critical personnel, and procedures to recover from a failed test. The system may be down for hours as failover and failback are tested. If there is no window in which this testing can be done, this complicates the testing process.

Aberdeen calculated the following statistics regarding the frequency of testing by organizations:

	Best in Class	All Others
Monthly	5%	0%
Quarterly	21%	9%
Semi-Annually	21%	19%

Clearly, this is an area of exposure for most companies. When the backup is really needed, there is no clear guarantee that it will perform as required if periodic testing is not done.

[2] Aberdeen also included server and storage virtualization, but it seems that virtualization technology is generally not geographically distributed and therefore does not play a role in disaster recovery.

Another area in the competitive assessment is the ability to meet data availability SLAs. This depends strongly upon the technology used to back up critical data. Aberdeen found the following usage statistics for backup technologies:

	Best in Class	All Others
Physical Tape	81%	58%
Replication	35%	30%
Managed Service	31%	13%
Virtual Tape	19%	13%

The leading best-in-class companies are more aggressively pursuing new technologies such as replication and virtual tape for the storage of their critical data. The advantage of these new technologies is the significantly reduced time to recover data and the reduction in the amount of unrecoverable data, thus supporting an improved recovery time objective (RPO).

Pressures for BC/DR Planning and Implementation

It is clear from the above study that companies have a long way to go to provide the protection that they need to recover from a disaster. Why after all these years of industry discussion on the subject are so many companies still unprepared?

To try to gain visibility into this question, Aberdeen asked what it was that motivated companies to pursue a BC/DR plan. The results follow.

Risk of Business Interruption	76%
Loss of Critical Business Data	51%
Recovery Time	32%
Preparation for a Future Event	20%
Regulatory Requirements	9%
Prior Business Interruption	5%

Evidently, these pressures are not being felt by many companies. It is interesting that only 5% of the respondents are reacting to prior interruptions. Perhaps this is because natural disasters such as hurricanes or tornados tend to occur only in specific regions. In contrast, companies in regulated industries such as financial institutions and government agencies are required to have formal business continuity plans.

Summary

Today's organizations, by and large, have a long way to go to ensure the survival of IT services following a disaster. The implementation, maintenance, and periodic testing of a BC/DR plan can be very costly; but this cost has to be compared to the cost of downtime following a disaster. The cost of downtime varies by industry but can range from thousands of dollars to millions of dollars per hour. In some systems, lives may be in danger. In any case, a long enough outage can put a company out of business as was proven by the 9/11 terrorist disaster.

Though not included in the survey, active/active systems provide the ultimate protection of IT assets. Should a node fail or be destroyed, services can be restored within seconds with little if any loss of data. Better still, if a passive backup system is already in place, the cost of moving to active/active can be very little. Best of all is that there is no technical testing of the backup plan required except for the ability to switch users or transactions to a surviving node – it is always known that the backup node or nodes are operational. BC/DR testing can then focus on the equally important problems of the relocation of people and their support services.