Better Backup Means Better Business Continuity

Secure backup enables companies to cost-effectively reduce the risk of data loss.

For 11 days in September and October 2010, Virgin Blue, the Australian arm of Virgin Airways, had to function at less than full capacity because of a data glitch. According to the airline, initial assessment of the interruption could impact pre-tax profit in the vicinity of $15 million to $20 million.

About a year earlier, the Florida-based Highpointe Hotel chain also had a close call when it suffered a hiccup on a main production server and thought it lost its redundant array of independent disks (RAID) system. This could have caused havoc with guest reservations as well as year-end financial data, payroll and general network files.

These two examples show the dependence that today's businesses place on data. Yet, many companies fail to establish business continuity plans, provide sufficient backup or adequately assess the risk that a data loss might have on their bottom line and their reputation.

A business continuity plan is a strategy for keeping a company operating even in the wake of a devastating disaster. Given the increased reliance that businesses have on digital assets, sound data backup and storage often are foundational elements in a successful continuity program.

STORAGE SOLUTIONS

Since documents became a key part of doing business, preserving records and documentation — in the event of a disruption — have been a vital part of assuring company longevity. Today, the enterprise depends on digital systems shared among employees, customers and suppliers. Documents are often updated in real time. And the risks have become much more complicated.

"Companies understand they have to plan for contingencies in the real world," says Lauren Whitehouse, directing analyst for the Enterprise Strategy Group. "However, frequently they fail to take the same precautions in the digital world."

When it comes to assuring business continuity, a company needs to manage its data and storage infrastructure using a four-phased approach:

1. Determine the true value of a company's system and data assets to the business.
2. Set a plan to optimize the existing infrastructure and evaluate technologies to fill any gaps.
3. Adopt a solution that prioritizes data availability based on its necessity to maintain business operations.
4. Establish a regular testing schedule of the plan and systems.

THE COST OF LOSS

The cost of a data loss or application downtime varies from business to business. But it's almost always a significant impact relative to the size and operation of the firm. "The cost of downtime is not a number anyone can pull out of a hat," Whitehouse says. "The cost is tied to the type of business and how it operates."

Mike Barton, offering manager in IBM's Systems and Technology Group agrees. "The total cost of any outage is hard to calculate in an interconnected world. However, the economic impact can be devastating for organizations that struggle with availability."

Businesses need to consider several factors when calculating the true cost of downtime. It's far more than just the lost revenues. According to Whitehouse, "Downtime costs should also include the cost of recovery, the cost of the disruption and the overtime spent getting back to normal operations."

Cost is often a significant barrier to implementing a solution. "CEOs and CFOs perceive disaster recovery solutions as costly and tend to hedge their bets," Whitehouse adds.

What that leads to in practice, says Michael Marchi, vice president for marketing at CommVault, is that CIOs often end up trying to manage and store data using the infrastructure that exists. Ultimately, that's a disaster waiting to happen, he says.

A BALANCING ACT

Instead, according to the experts, business chiefs should shift their thinking. They need to adopt a middle-of-the-road approach that leverages the existing infrastructure to do things differently. They also need to deploy new technologies, such as deduplication, to establish a viable recovery posture.

This approach makes sense from a cost perspective. But given the recent tough economy, many businesses report that their existing systems are stretched thin and are struggling to cope with increasing data storage and access demands.

"Everyone's budgets are understandably constrained," says Teresa Worth, a senior product marketing manager at Seagate Technology. "But an IT organization simply cannot afford to fall behind and risk data loss or information breaches. In some cases, data loss can mean the end of the business."

Although cost might be a barrier to adopting new storage solutions for business continuity (BC) and disaster recovery (DR), demand for storage continues to increase rapidly. Globalization, data center consolidation and data-generating applications combine with data retention mandates to fuel demand — no matter the economic climate.

"Global organizations face two conflicting trends in terms of storage and business continuity," says Lee Johns, director of marketing for unified storage at HP's StorageWorks division. "The first is centralization to fewer data centers" to reduce operational overhead and management burdens.

"The opposing force is the massive user generation of data and the desire to keep active data as close as possible to users," he adds. "That drives smaller decentralized storage solutions, which can be more difficult to back up."

IBM's Barton agrees: "Globalization is one of the forces causing organizations to rethink their strategies for maintaining information availability. For most organizations today, the question isn't whether to provide 24x7 information availability but rather how to do it most effectively."

INNOVATION CREATES OPPORTUNITIES

Establishing a working BC/DR strategy requires an investment of both resources and money. The overall cost, however, has recently dropped dramatically. For many CIOs looking at BC/DR in 2011, there are substantial reductions in the investment required compared to 12 months ago.

"It's easy to spend too much money on infrastructure and people, or spend too little and put information at risk," Barton says. "The good news is, it's getting easier and less expensive to support 24x7x365 availability, even for midsize organizations."

The technology behind BC/DR and storage solutions has evolved to automatically perform the tasks in a much smarter way than previously possible. Business disruption is minimal, with systems able to failover to alternate DR sites without users or customers noticing.

Recent technology developments directly affect the resources required for both storing and managing data and applications as well as recovering them should disaster strike. "The technology for managing data and how we recover it is much more cost-effective," CommVault's Marchi says. "Even when leveraging existing technology, we can manage things very differently."

New technologies that are expanding BC/DR options include:

- Replication with deduplication
- Faster, less expensive tape drives and libraries
- More effective backup to disk
- Storage and file virtualization

- Continuous data protection (CDP)
- Infrastructure and network connectivity options
- Innovative tools to back up Microsoft Exchange Servers and BlackBerry Enterprise Servers

Keep in mind, choosing the right mix of tools is more than simply comparing and contrasting hardware and software. A thorough review of business processes is required, with particular attention paid to determining what constitutes mission-critical, business-critical and noncritical data and applications. Plus, it's imperative that a business also accounts for the people and resources that drive them all.

"A disaster recovery impact analysis should be undertaken by every business," Whitehouse says. "The idea is to see what would happen, the alternative actions that would need to be taken, in addition to the associated costs to the business."

What constitutes mission-critical information depends on the individual company. "Determining what is important will vary widely depending on the particular business," says Marchi. "Companies need to determine where they make their money, and the systems which drive that, so they can assess what is absolutely mission-critical."

For instance, he notes, a company might rely heavily on e-mail systems. However, it might not need them to maintain operations, even though their loss will certainly affect productivity.

"In this case, it's better to classify e-mail as a business-critical application rather than mission-critical," Marchi notes. On the other hand, an order-tracking application might contain data that users need to process transactions. That is clearly a mission-critical system.

The upshot? Businesses will need to determine which applications and data are truly necessary for business operations and which less so. Marchi suggests using an acid-test question: "How long can you last without the data and/or application?"

MEASURING AGAINST A POINT IN TIME

There are two measures that a company can use to help evaluate viable solutions. These are the recovery point objective (RPO) and the recovery time objective (RTO).

"The recovery point objective is the point in time you want to be able to recover from," Marchi says. "The recovery time objective is the amount of time to recover from a disaster recovery event."

The RPO determines the cost of a solution, while the RTO can reduce that cost if the business can stand the pain of being without its data and applications. "There is a balance to be struck," Marchi says. "The tradeoff between RTO and RPO is challenging for most companies."

Classifying data and applications based on how critical they are is the key. More important applications and data should be backed up more frequently, probably several times a day to reduce the RTO. These should be classed as mission-critical.

Less critical data, such as e-mail, may need backing up once a day; these would constitute business-critical elements. Noncritical information, such as records kept to comply with regulatory retention rules, can be backed up using less-expensive storage media or off-core systems entirely.

The benefits of a holistic view to data storage and backup are clear regardless if a firm ever experiences an outage. Reduced management time, lower storage needs and a simplified interface mean less staff time devoted to running the system — and that means lower operational costs.

[SIDEBAR 1]

10 Business Continuity/Disaster Recovery Best Practices

1. Define requirements for DR: Assess infrastructure size, physical and geographical diversity and project revenue loss, recovery loss and opportunity cost.

2. Conduct due diligence: Assess current infrastructure, applications and data, and classify each as mission-critical, business-critical or noncritical.

3. Identify recovery time objectives and recovery point objectives: Determine the RTO and RPO for all mission- and business-critical components.

4. Maintain secondary backup copies: Establish an offsite DR facility and keep it current at all times.

5. Assure data availability: Provide ability to access data even if access to the data center becomes unavailable. Maintain the ability to restore critical files from a DR site.

6. Choose a trusted partner: Consider using an external DR provider to expedite recovery.

7. Use replication technologies: Adopt replication tools to facilitate creation of offsite data copies and provide multiple recovery points.

8. Automate restores: Speed server recovery through automated restore capabilities.

9. Document the DR process: Provide full documentation for all DR procedures.

10. Test, test, test: Conduct regular reviews, including full-blown dress rehearsals.

Graphic:

o 93%: Businesses that had to use their disaster recovery plans

o 3-to-4 hours: Average time spent recovering from a disaster

o $287,000: Average cost of a disaster recovery incident

Footnote> Symantec, Disaster Recovery Survey — Global, June 2009

PULL QUOTE

"When a disaster recovery event occurs and your strategy goes into action, you want to be humming along, not hobbling along." — Michael Marchi, Vice President for Marketing, CommVault

EL PUNTO

47% Business technology managers who say they don't have the resources to recover critical business applications and data

SOURCE: Information Week's "2010 State of Enterprise Storage Survey" of 331 corporate IT chiefs

CONSULT WITH YOUR CDW ACCOUNT MANAGER AND CERTIFIED STORAGE SPECIALIST TO SELECT AND LEVERAGE THE RIGHT BACKUP SOLUTIONS.

121510