Best Practices: Backup and Recovery Strategies

Computer Associates International, Inc.
Published in Partnership with Inc.
June 2005

Best Practices:
Backup and Recovery Strategies

You can't recover data that you haven't kept. But how confident are you that the data on which your business depends is backed up successfully? This paper examines the kinds of data storage technologies and solutions that are best for all businesses and offers some best practices for ensuring the successful data backup and recovery required to sustain operations — regardless of what happens to your business.

What Causes Data Loss?

Hardware failure	40%
Human error	29%
Software corruption	13%
Theft	9%
Computer viruses	6%
Hardware destruction	3%

Source: David M. Smith, Ph.D., Pepperdine University, 2003

It's always a challenge to keep your business data readily available when you need it. And this job gets even tougher the smaller your technical staff — assuming that you have a staff at all.

Managing and Minimizing Storage Requirements

To meet your growing data storage demands without suffering through repeated upgrade hassles, it's worthwhile to stop and carefully review your:

- **Current and anticipated storage requirements.**

- **Data protection and backup needs**, since backing up multiple servers, volumes, and desktop systems can quickly get very complex.

Cost-effective Data Storage Solutions
The cost of data storage has plummeted in recent years. Meanwhile, the labor costs associated with managing data storage keep climbing. So consider buying more storage — even more than you think you'll need. It's worth it in the long run and the extra cost is negligible.

To keep storage management costs in line, think hard about how you'll configure your data storage. For instance:

- **It's probably not worth upgrading the storage built into your existing servers** since the cost of backing up the data they contain, adding new hard drives, then restoring the data will be substantial. Instead, make sure that the data storage you do buy is scalable, so it's easy to add more later when you require it.

- **Buy the kind of data storage devices best suited to the services they support**. For instance, IDE drives usually work just fine for file and basic application services, as do SATA controllers and drives. While IDE and SATA devices can't match the performance of SCSI drives (which offers fast transfer rates and rotation speeds), they cost much less than SCSI solutions. For applications requiring high-performance and reliable availability of data, look to SCSI RAID solutions, which cost more but deliver fault tolerance with redundant configurations (how much availability and fault-tolerance depends on what sort of RAID level you select).

- **If your data is stored on multiple servers**, you can consolidate it onto fewer servers with larger hard drives so management and backup is easier.

- **If you need to add storage to your company network, consider NAS** devices, which are simpler than file servers since they use web-based administrator interfaces to mask operational complexities. Pay close attention to NAS device details to ensure that your chosen solution works with your existing systems and networks while remaining scalable.

- **If you need high-capacity, undisrupted data access, redundant system links to ensure data integrity, an ability to reconfigure and/or scale your storage infrastructure, and centralized storage management and backup capability**, consider a SAN. iSCSI-based SANs, which are based on IP-friendly Ethernet network technology, are less expensive and complex than Fibre Channel SANs.

Tips for Taking the Backache Out of Backup

As your business increasingly relies on data, backing up that data becomes even more important but also more complex. The effort can be grueling (and costly) if you do not have a backup strategy that is based on proper planning and is faithfully executed according to a carefully crafted backup policy. Here's how to begin:

- **Decide what you need to back up**. Start with your answer to "What can we afford to lose?"

- **Understand your data environment**. Once you know what requires backing up, you'll need to determine the systems and hosts where it's located; what type of data it is; how often it needs to be backed up and how often it's likely to be retrieved/restored; how long it must be retained and in what form; how much time you have to complete the backup; and what kind of security the data requires. By ranking the importance of your data and eliminating the unnecessary data from your backup efforts, you can save storage space.

- **Find the backup techniques and technologies that best align with your business needs and that automate as much of your backup efforts as possible**. For instance, it may be worthwhile to consolidate data on fewer servers to reduce backup management efforts. You may benefit from using backup/recovery solutions that are bundled with a storage appliance. Or perhaps you should opt to outsource backups entirely. Consult with an expert if you don't understand this process.

- **Craft the processes and procedures you'll need to ensure backups are completed properly,** including assigning responsibility for getting backups accomplished and monitoring the effort to spot problems, while also ensuring that those responsible are sufficiently trained.

- **Ensure that backup copies are valid and can be successfully restored**, which requires that you rank the importance of your data and establish ways that the most important data is backed up first and restored first. Be sure that you have adequate time to back up all the data that's important to your business, and be sure to understand the time required to restore that data in case of loss or corruption. You'll also need to regularly check and test your equipment, media, and processes.

- **Ensure that backup copies are safe**. Generally, this means storing your backups in a logically and physically secured offsite location. It also means ensuring that you haven't backed up viruses and other malware, spam, and data that is not important or that is harmful to your business.

- **Maintain backup logs** so you — and your auditors — can track backup activities.

- **Regularly revisit your backup/restore risks, procedures, and technologies** to make sure they are adequate as business needs and conditions evolve.

- **Dispose of backup media carefully**, making sure that they are physically destroyed so that their contents cannot be read by the unauthorized.

Of course, the backup technologies you use depend greatly on the size and nature of your business and how it uses information. Below are some newer technologies that may be able to help ease your backup burdens.

Best Practices for Business Continuity Protection

The ability to sustain business operations in the face of disaster — or merely a hardware or network failure or employee error — requires planning.

You can figure out if the effort is worthwhile by asking and answering one simple (yet scary) question: "How long would my business survive without its computer systems, networks, and applications; without its business data; without its phone system; and without its offices?"

If you conclude that it's wise to think through how your business should respond to events that interrupt its operations, you can begin with the guidelines contained in the DRBC (disaster recovery/business continuity) Framework, developed by Naresh Malhotra and Saby Mitra of the DuPree College of Management at the Georgia Institute of Technology:

• **Charter a team**. This involves getting commitment from the CEO of your company and establishing a cross-functional steering committee and a core operational team.

• **Conduct an analysis of your business**. You'll need to identify the goals of your business as well as its outputs, processes and resources, the risks it faces, the potential impacts of those risks, and the roles of those (such as technology vendors) you'll turn to for risk mitigation.

• **Define a disaster recovery/business continuity strategy**. This must be done at the company-wide level as well as for your business processes and resources; then you'll need to figure out how to pay for it.

• **Develop a detailed plan**. Define its scope, document requirements in detail, then design it.

• **Implement your plan**. Steps include getting buy-in throughout your company, developing implementation documentation, assigning roles and responsibilities, training employees, and testing what you've implemented.

• **Maintain your plan**. You'll need a change management process as well as the ability to monitor performance and benchmark new applications, products, and processes.

This effort may not have to be as complicated as it sounds. Businesses often can, for instance, get help setting priorities at facilitated workshops that conduct risk assessment and business impact analyses. If your business has multiple locations, one site can serve as backup for another. In addition, you can upgrade your IT systems maintenance contracts to get replacement hardware in 24 to 48 hours, which can be drop-shipped to a recovery location where data and applications can be loaded from backup stores.

The key is planning, training, testing, and regular review of the plan. Do this and you'll have the same chances of surviving any trouble that you might encounter regarding your business operations.

For more information on CA's small and medium business solutions, please visit ca.com/smb.

Quality System ™
Quality
Endorsed
Company
ISO 9001
Lic. 2443

ca
Computer Associates®

MP282990605