

Data Protection Planning

Tips for successful Planning

Faced with unrelenting data growth in accounting, document management and e-mail, today's IT administrators find themselves increasingly pressured to ensure the availability and security of their digital assets and to be able to recover quickly from anything from a simple drive failure to a more catastrophic data loss.



But imagine how difficult it is for firms to do this without a formal IT staff—just one person who sets up PCs and swaps out backup tapes while trying to keep up with regular job duties? Strapped for IT resources, these firms often don't set up procedures for how most securely and cost effectively to manage the data backup and recovery processes; rather, they're hampered by such technical limitations as being unable to take advantage of incremental backups that shorten backup windows and enable less data to be stored on spinning disk or tape; having to rely on manual transport of backup tapes instead of leveraging existing network infrastructure where data can be electronically sent to a secure, offsite data center; and if the firm has offices, having to employ a redundant backup infrastructure instead of a centralized one.

For a firm to maintain business continuity, the following — corporate policy, technology and other considerations—should be addressed.

Corporate Policy

Identify, prioritize and protect the company's most important current applications, and forecast which ones will be needed in the future.

As data grows and resources remain static, design a plan that simplifies and automates IT functions. Policy-based automation not only maximizes resources, it limits human errors that, according to the Gartner Group research firm, account for about 40 percent of failures.

Centralize backup management. Having common practices across offices ensures operational efficiencies related to capital outlay and manpower resources.

Don't recreate backup policies every year for new areas or growing areas. Rather, standardize policies and make them pliable enough to work as the firm and its digital assets grow.

Technology

A data protection and recovery plan requires flexibility to leverage existing infrastructure with cost effectiveness and be able to account for future growth in personnel, amount of data and number of offices.

Other Considerations

Return to Operations. How much downtime can the firm tolerate before it significantly impacts business?

Offsite Storage. If your region has a propensity for natural disaster, does it make sense to get data quickly offsite to a secure data center facility out of the area?

Data Recovery. What are the procedures for getting the digital assets from storage? Who will do this? Identifying and prioritizing business-critical applications will make it easier to decipher what data to restore first.

Security. Does the backup software have a self-encrypting process? Are firewall appliances being used? Consider the owner and location(s) of encryption key(s).

Vendor Evaluation. Look to professionals with a proven track record of helping other firms. Talk to others within your local area. Be cautious of organizations who simply want to throw more equipment and money at the problem.

By addressing these issues, you will be taking a big step towards establishing a viable data protection and recovery plan—regardless of the size of your firm or IT budget.