CENTRAL VS. LOCAL STORAGE: WHAT IS RIGHT FOR YOUR GROWING BUSINESS?

As small companies grow, they face an increasing number of IT challenges. Two of the most critical are:

- How to back up files and ensure that mission critical data is always available when it is needed, and
- How to protect customer privacy?

Central to each of these questions is where should data be stored? Should it reside on local disks on client computers or on a shared network storage device?

The former happens almost by default. Today's modern desktops and notebooks ship with a significant amount of storage capacity. It is not uncommon to find desktops with disks larger than 500 GB. Even the least expensive netbooks feature 160 GB disks. With so much storage capacity available, it is easy to slip into the belief that data should be stored on local disk drives. After all, both the Windows and the Macintosh operating systems support simple file sharing and provide security with user logins and passwords. But, while peer-based shared storage does provide rudimentary file sharing that might seem like a good solution in a small business environment, storing business data on local desktop computers is fraught with a number of risks:

- Client computers may be compromised by computer viruses that can corrupt or destroy data.
- Client computers are not fault tolerant. If the single drive found in most computers should fail, company data that is not properly backed up could be lost. A recent study by Google indicates an average of 1.7 percent of hard drives fail within a year, and that over 8.6 percent of three year-old drives failed.
- Client computers in offices and cubicles are rarely physically secured. A knowledgeable intruder could easily compromise and destroy data. And, if not physically secured, a desktop or laptop could be stolen.
- Should locally stored data reside on a notebook used by an employee who travels frequently, the risk for theft or loss increases. A recent Ponemon Institute study sponsored by Dell discovered that up to 12,000 notebooks are lost *weekly* in airports. Highlights from this study show that 53 percent of business travelers surveyed said they carry sensitive corporate data on their notebooks. Forty two percent of the respondents said that they do not backup their data. Amazingly, 65 to 70 percent of notebooks are never reclaimed.

To avoid these risks, small businesses should develop a centralized data storage policy. The benefits of centralized storage include:

- All corporate files can be stored on a common device that can be backed up by centralized backup software and/or hardware.
- Files stored on in a central location can be shared with other individuals and groups, or can remain private for individual users. This eliminates the "sneaker net" of sharing files on USB flash drives.
- With files stored in a centralized device, it makes good economic sense to invest in fault tolerance for that device. Fault tolerance could include a RAID array for data redundancy, as well as an uninterruptable power supply (UPS). In most companies, it is not economically feasible to build fault tolerance into each client computer.

- Centralized storage is easier to physically secure than all of the client computers.
- It is far simpler to manage data access policies when all of the data is stored in a centralized location. Once the number of computers exceeds four or five on a peer-to-peer network with shared folders, managing the decentralized data stored on those computers quickly becomes an impossible task.
- Consolidation of company data into a centralized location optimizes a company's investment in storage. Storage on centralized devices is better utilized than the storage capacities on client systems. The investment in fault tolerant centralized storage can usually be at least partially offset with savings achieved by purchasing client systems with minimal hard disks.

A centralized storage strategy involves choosing a centralized storage platform. There are essentially two choices: A server-class computer with a general purpose operating system, such as Microsoft's Windows Server products, or a Network Attached Storage device (NAS), which is optimized for storing and serving files. Both storage platforms can provide the benefits of centralized file storage, but each presents unique advantages and disadvantages.

Some applications, such as Microsoft's Exchange server for email as well as some database applications, must run on a Microsoft platform. These applications require block-level access to their respective data stores. In the simplest installations, that data store is often the Direct Attached Storage that is part of the server. Deploying a Windows-based server usually requires either an IT professional or, for companies too small to justify a full-time IT staff, a Value Added Reseller (VAR) for set-up and maintenance. These servers require the installation of regular patches from Microsoft, as well as installation of anti-virus protection, both of which drive up the total cost of ownership (TCO).

Many small businesses may not need server-based applications such as email. Often, their mail is outsourced to an Exchange provider or they rely on POP mail from providers like Google. For these companies, a NAS device could be the perfect solution to providing centralized storage. NAS products deliver all of the benefits of centralized storage but have a number of advantages over conventional Windows-based servers:

- NAS devices are available in many different configurations. For NAS products with more than a single drive, fault tolerance is built into the platform using various RAID configurations. Typically, depending on the RAID configuration, data will be preserved even if one or more drives in the drive array fail. Hot swappable drives, a feature on many NAS devices, allows for the removal and replacement of a failed drive without powering down the NAS device. This eliminates downtime.
- NAS devices typically operate on a Linux operating system that provides several advantages:
    - Linux is a stable operating system that rarely requires patching.
    - It has no licensing fees, thus offering a TCO advantage.
    - Viruses and other malware rarely target Linux.
    - The NAS operating system runs in flash memory that cannot be infected by viruses.
- NAS devices are easily configurable by non-IT professionals. User-friendly web interfaces and installation wizards ensure that a NAS can be fully operational in about 15 minutes, again lowering TCO.
- Additional storage capacity can be added to an existing network by deploying a NAS. Since the NAS device is being added to the network, there would be no downtime as might be experienced when adding storage capacity to a Windows-based file server.
- NAS devices can integrate into an existing network environment.

- With built-in active directory support, a NAS can be configured as a storage device in an existing Windows network.
- Many NAS products now support iSCSI, an IP-based standard for connecting storage devices. Some or all of the capacity of the NAS can be defined as an iSCSI target. Clients, including servers, using an iSCSI software "initiator," can connect to an iSCSI target and have block-level access to the NAS data store. The NAS appears as a local drive.
- Virtually all NAS products provide cross platform support for Windows, Macintosh and Linux/Unix clients. No special configuration is required.

For small to medium businesses, centralized storage offers a number of advantages over a distributed storage model. But today's NAS products provide a very cost-effective and scalable alternative for centralized storage. Thus, it should be a part of the storage strategy in any growing business.