ITS FOLDER SHARES AND PERMISSIONS

NTFS partitions allow you to assign file and folder permissions to resources. Typically, there are two ways of accessing data files the first is through a network share, and the second is through direct access on the machine. Because of this there are also two areas where the permissions can be applied, share and folder (file).

The share permissions consist of:

Read – Users can **Default for Windows XP and 2003 Server
- View Files and subfolders
- Access any subfolders
- Read file data and attributes
- Run program files

Change – Users have all Read Permissions and can
- Create files and subfolders
- Modify files
- Change attributes on files and subfolders
- Delete files and subfolders

Full Control – Users have Change permissions and can ** Default Windows 2000
- Change file and folder permissions
- Take ownership of files and folders

These permissions are cumulative. If you are a member of a group that has read permission and a second group that has full control permission then you would be using the least restrictive permission (Full Control) then you would look to the File/Folder Permissions.

The file/folder permissions are similar:

Read – Users can
- View Files and subfolders
- Access any subfolders
- Read file data and attributes
- Run program files

Read & Execute – All Read permissions and
- Ability to run programs

Write – Allows users to
- Create and edit files
- Create and add to folders

Modify – All Read & Execute and Write permissions also
- Ability to delete files

Full Control – Rights to do everything to the Files/Folders

These permissions are also cumulative. If you were a member of a group that had Read & Execute permissions and a second group with write permissions then you would have all the rights and privileges of those two permission levels.

If you are accessing the data directly on the machine then only the file/folder permissions apply. Otherwise you would compare the highest level of access allowed by the share permissions and the highest allowed by the file/folder permissions and use the ***MORE*** restrictive of the two.

How to apply Permissions:
Microsoft's best practices for apply permissions are:

1. Create a user account
2. Create a security group
3. Place the user into the group
4. Apply permissions to the group

If you only have to administer one or two users you may not decide to do this, but for more it does reduce administrative overhead. If there are ten users who need the same level of access to five different resources, you could apply the permissions to each account on each resource (50 changes) or add them all to a group and apply the permissions to the group (5 changes). If one of the people changes departments, just remove them from the group and done no security permissions need to be modified. If a new user comes in you don't have to remember all the folders they will be access to, just add their account to the correct group and the administration is done.

For administration of shared resources it is typically easier (although slightly less secure) to give Everyone Full Control of the Share Permission and control access to a resource via the File/Folder permissions. (You can also use Authenticated Users or Domain Users instead for added security.) You then only have to modify one set of permission to give access to the resource.