PO Box 3146
Alpharetta, GA 30023
(770) 951-2080
www.cyberscrub.com

Practical Uses of CyberScrub Technology to Ensure the Secure Deletion of Data

This paper will touch briefly on the practical applications of deploying CyberScrub products and technology to 1) wipe free and slack space on hard drives and 2) to affect the transparent secure erasure of selected files and folders through standard keyboard interaction.

Wiping Free Space

Data that has been deleted through the normal course of events (i.e.: using the Delete key or accessing the right click context menu>Delete) is, without going into a detailed and technical study, almost universally recoverable. “Delete” does NOT mean “Erase”. Regardless of whether the data goes to the Recycle Bin or bypasses this staging area (by utilizing ALT>SHIFT>DEL) the net effect is a renaming of this selected digital asset, resulting in the obfuscation of such information. The resulting consequence is that the “deleted” file is simply designated as an available area in which to place new data. Even in the event that the previously “deleted” file is overwritten, in most every instance there is still a strong likelihood of partial recovery, as the new data rarely fills the full area previously occupied by the previous file. This “file slack” is cause for considerable concern.

Wiping free space is the process by which all deleted files (i.e.: those files that have been marked as space available to be overwritten) are methodically overwritten or “wiped” with proscribed or random data to make the original contents non-recoverable. An analogy would be a word written on a schoolroom blackboard. To prevent the discovery of the blackboard contents, a student may take chalk and write a continuous series of additional and random characters over the original word, making its discovery impossible.

However, wiping free space is, especially with large drives and secure overwriting methods, a long and arduous task. CyberScrub provides solutions that allow the wiping of free space to occur when the computer is idle, similar to the activation of a screen saver. This allows for the passive implementation of disk wiping without the inconvenience of placing the active, in-use computer out of service, even temporarily. This type of implementation may be initiated at any point of the computer life-cycle to ensure that the legacy data residing on the targeted drive is securely erased and non-recoverable.

Effecting Secure Erasure from the Initial Deletion

By utilizing powerful CyberScrub scheduling capabilities, data that has been insecurely deleted from standard keyboard actions can be securely erased from the Recycle Bin automatically, based on time or event parameters. To ensure and enforce established records policies, data retention options may be easily incorporated to restrict such automated Bin erasure to pre-determined document life cycles. For example, secure erasure of Bin contents can be restricted to items greater than 30 days. Additional

options allow for the use of masks and filters to qualify such contents for the specified destruction actions.