

Identity Theft Lurks In Your Copy/Printer Room!

Any device that temporarily stores data on a hard drive or any storage media for that matter will have some residue left behind after the file is removed. On most modern copiers and scanners, files are temporarily stored or queued to a storage device such as a hard drive or flash drive. Once the process in progress completes (e.g. the file is printed) the queue manager will delete the file. However, in most cases the file isn't securely deleted. It is actually just marked as deleted so that the file system can reclaim the space occupied by file.

The Problem

Most file systems handle file deletion by marking the file as deleted but don't by default delete the contents of the file. This is intended to make data recovery easier so that if the drive starts to go bad or you accidentally delete a file you can still retrieve its contents. There are many freely available tools to "Undelete" files from a windows NTFS or FAT file system. And before anyone (like me) starts to assert that Linux and Mac/OSX file systems don't have that problem, they are susceptible to this problem as well. Basically, if data has been written to the storage device there are tools out there that can be used to recover some percentage of the data that has been "Deleted".

The Solution

There are many possible solution sets to help address this problem. Like most technology related problems the solution sets fall into three categories: People, process and technology ... in that order.

People

One of the best solutions is to educate the people in your organization on how to handle confidential information. For example, printing off your customer address book at the local copy store probably isn't the best way to protect your customer's identity data.

Process

Business processes and procedures are to be focused on secure printing and photocopying practices. In some cases, this means that security sensitive information never leaves the work premises whether in electronic or printed form. In others it may mean that all security sensitive information is only printed on the printers with encrypted drives. In others it may mean that no one can photo copy security sensitive information on public copiers.

Technology

Even though people and process are a huge component of any solution, most people run to technology to solve these sorts of problems. Fortunately, technology can help. Here are a few pieces of technology to consider.

Encrypt the Data

Consider purchasing the encryption option for your printer or copier. This option encrypts the data before it is stored on the storage device. If the device is ever stolen or copied, the probability of someone recovering the data from the device is very low. As the CBS video points out this option may tack on another \$500 to your printer or copier. However, consider the risks that you run if the data contained on the storage was ever compromised.

Encryption can also be applied to the desktop as well. There are many solutions for Windows, OSX, and Linux for encrypting the full disk drive or a partition of your hard drive to ensure that the drive is ever stole, the data cannot be recovered. TrueCrypt is a great open source and cross platform solution that works very well for this purpose.

Cleanse the Media

Businesses should institute a standard operating procedure to cleanse all equipment when retiring any and all storage media. To cleanse media is to wipe the contents off in such a way that it can never be recovered. My favorite tool of choice is Darik's Boot and Nuke (a.k.a. DBAN). With DBAN, you can apply military grade cleansing to just about any disk media. Disposing of other media should be done secure means as well. For example, shred DVDs, CDs and tape with a high grade cross-shredding device. Don't just throw them away.

Control Access

Probably the simplest thing that can be done is to control the access to your printing and copier devices by putting them in a locked room. Don't let people use those devices unless they have permissions to use them. Most business class photocopiers and printers also support electronic control as well by requiring a user to login before they can print or copy a document.

Note that access control also applies to the electronic domain as well. Companies would be wise to apply secure access controls to internal web sites, file shares, and backup repositories. Oracle offers a full platform for enterprise wide and web access controls, single sign-on and federation through their identity management suite.

Dispose Securely

When disposing of printers, copiers, computers or anything that might have a storage device, be sure to wipe the data before getting rid of the item. If you don't know how to wipe the device yourself, find someone that you trust that will do it for you. This goes for papers as well. Have a locked storage bin that people can easily throw away security sensitive information into. Then securely shred the contents of those bins on a regular basis.

For further information, please contact your OSP Risk Management representative.