



» STEVE KNUTSON
Chief Information Officer
Marco
www.marconet.com

Copiers Pose Security Risk

BUSINESSES HAVE LONG recognized the vulnerability of computer hard drives and have implemented a series of practices in the name of security. But these are not the only electronic devices that could compromise an organization's sensitive information.

Consider for a moment what your organization has printed, scanned or copied in the last year. What if that information got in the wrong hands? Would it compromise your company's security or the privacy of your customers?

Today's digital copiers or high-end laser printers may store images of scanned, faxed and printed document. That comes at a surprise to some business leaders who never realized these devices had hard drives.

Recent media coverage on copiers and printers scrapped for parts in foreign countries raises questions about what companies do to protect any sensitive information stored in the hard drives of copiers or all-in-one printers. When left in the wrong hands, the hard drives filled with personnel files, financial reports and personal client information can put organizations – and their customers – at risk of identity or data theft.

Guarding the data is the responsibility of the organizations before disposal. Technology companies and the device manufacturers have a series of policies and programs in place to help organizations protect security and privacy of the scanned, printed and copied files. Yet, according to recent reports, the majority of companies do not properly handle the hard drives before disposal.

Here are three steps organizations can take to prevent a security breach:

- **Secure**

Before organizations remove these devices from their

workplaces – or call on a company to handle the disposal – they need to assess if the device contains any sensitive information. In some cases, the printer or copier contain information that is not personal or the information has been encrypted to a level they are comfortable with.

In these instances, businesses can leave the hard drive intact pursuant to the current policies of the manufacturer and technology provider handling the disposal. This is often the case with copiers designed for public use.

- **Overwrite**

By overwriting a hard drive, organizations essentially scrub the hard drive clean of the information. Then, they can leave it in the device before it is sold to a wholesaler. Software, commonly used by companies like Marco, is available to systematically pull all the information off the hard drive.

Technology providers typically perform this safeguard upon request for a fee. Large companies sometimes purchase the software to have their information technology department overwrite their devices.

- **Remove**

The most secure method of handling an unwanted hard drive is removing it from the device and destroying it. Organizations also can choose to have a technology provider remove the hard drive and leave it with them for safe handling.

These steps do not require much time or money and will go a long way in preventing misuse of an organization's information. Businesses can reference the manufacturer's information and enlist a local office technology provider to aid in the process.