

A new threat for identity theft - your copier!

By Robert Slayton, CITRMS

BACKGROUND

Newer copiers are the latest bonanza for identity thieves. Most digital copiers manufactured in the last five years contain hard drives that store all copied pages. These hard drives (similar to the hard drive on your computer) were added to increase the functionality of the copiers and also allow users to print directly to the copier. Every page that is copied on a digital copier is stored in this hard drive and is accessible to identity thieves or business competitors. Manufacturers have only recently started development on systems that will either encrypt the hard drive or wipe the information clean once a job has been completed. Sharp was one of the first companies to alert the public to this risk of a security breach.

TAX SEASON MEANS COPIERS ARE A PRIME TARGET

Many employees use the business copier to copy their personal tax returns. If this information falls into the wrong hands, would your company be liable? Under the Fair and Accurate Credit Transactions Act (FACTA), companies are responsible for protecting both employees' and customers' non public information. If it is determined that not safeguarding your copier's hard drive was negligence, then you would be liable for restoring that person's/customer's identity and paying for the actual losses. According to the Federal Trade Commission, the average amount of time it takes to restore a person's identity is 600 hours. According to an article in CIO Magazine, actual losses are typically between \$42,000 and \$92,000.

What other confidential information has been placed on the glass to make copies for other employees? Just because a copier is locked up in HR or an executive's office doesn't mean it is safe. A tech savvy person on the cleaning crew or disgruntled employee could easily download this information. Imagine the wealth of sensitive corporate and competitive information that is available on one of these hard drives.

RECENT COPIER UPGRADES

If you recently upgraded your copiers and traded in/sold the old ones, then you are still at risk. Your business information could still be stored on that old hard drive, much like selling an older computer without wiping its hard drive of information. If you plan on purchasing a digital copier with a hard drive, then make sure it either encrypts the data, overwrites the information, or has another tested security mechanism.

IMPACT ON INDIVIDUALS

First, if you use a public copier, you could be at risk. Ask before copying to see if your information will be stored on the copier after you leave. Second, talk to your tax preparer. They usually make copies of your tax return so make sure that they are aware of the risk and ask what steps they are taking to prevent a breach of data. Third, be vigilant ANYTIME that your personal information will be exposed, whether on a copier, over the phone (or cell phone), instant messaging, and internet to name several.

SUMMARY

Copiers are just the latest item in a long list of ways that an identity thief can steal your business and personal information. Be careful when using a copier to copy personal or sensitive business information.

Robert Slayton is a Certified Identity Theft Risk Management Specialist who consults with businesses and individuals on how to minimize their risk of identity theft and provides identity theft prevention and restoration services. For more information on his services or free information on how to minimize your risk of identity theft, contact him at Robert@robertslayton.com or call him directly at 1.800.913.2378. Robert manages a full service insurance agency, Robert Slayton Associates, out of Naperville, Illinois.

©2007 Robert C Slayton