

How Your Old Photocopier Can Cause a Security Breach

According to, “Digital Photocopiers Loaded with Secrets,” published on CBSNews.com, nearly every digital copier built since 2002 contains a hard drive, much like the hard drive on your personal computer. The copier hard drive stores an image of every document that has been copied, scanned or emailed by the machine.

The security risk occurs because an estimated 60% of Americans do not realize that the copier has a hard drive, and therefore, never sanitize it before selling, giving away or swapping out their current photocopiers. That means would-be thieves simply need to download/print the contents of a copier’s hard drive to gain access to literally thousands of documents – many of which could contain confidential information.

Think this threat isn’t credible? In February 2010, CBS News investigated the photocopier hard drive issue firsthand by going to a warehouse in New Jersey, where they purchased four used printers. It took an IT security expert only minutes to remove the hard drives, run a widely available forensic software program and then download tens of thousands of items in less than 12 hours. The results of the investigation were shocking – domestic violence complaints, pay stubs and even detailed medical records with names, prescriptions and diagnoses. If these documents fell into the wrong hands, not only would they potentially expose innocent victims’ personal information, but also the company that mishandled the printers could receive serious monetary fines and damage to its reputation.

With the seriousness of this threat in mind, what should you do to prevent a copier-related security breach?

- **Destroy the hard drive.** If a photocopier is slated for an upgrade or removal, have an IT professional remove the hard drive and destroy it thoroughly and securely.
- **Consider encryption hardware.** Most copier manufacturers offer security or encryption packages that render the hard drive information unreadable.
- **Explore specialized products.** There are photocopiers products on the market that automatically erase an image from the hard drive, as opposed to storing it.

In addition to these specific precautions, your company can also explore more general practices to improve its overall security that include:

1. Document all information security risks specific to your organization - consider both paper-based and electronic information sources. Of particular importance is data generation, storage, transfer and the information destruction process.
2. Develop/implement policies that control employee access to confidential information.
3. Train your employees in best practices in secure information management and destruction.
4. Destroy all confidential information - in electronic and paper form – after legal retention periods are met.
5. Explore outsourcing information destruction to reputable, professional providers. A high-quality provider can ensure the total security of the information destruction process, and can provide documentation to certify that the chain of custody has been maintained and the work has been completed.

With these tips in mind, you’ll be on your way towards creating a company culture that values and emphasizes the importance of respecting an individual’s privacy. Additionally, by being aware of specific risks such as a photocopier’s hard drive, you can then take proactive steps to incorporate such risks into your comprehensive security policy – creating a better and more secure workplace for employees and customers.