



MFPs & Privacy Issues

Dealers must reassure & educate their customers

by: Mike Arnold, CPO Ltd.

Ask any office equipment dealer what his (or her) greatest challenges are and you will probably get the same answer: tightening finances and the accompanying drop in sales because business owners are being more cautious with equipment purchases and leases. Without question, those are serious issues, but we face another challenge on the horizon: potential threats to individual privacy courtesy of the office copier/MFP.

Few have previously regarded the office copier/MFP as a threat to privacy and identity protection. In fact, a survey that grew out of a CBS Evening News report on the topic of hard drives and copier/MFPs showed an alarmingly small percentage of the population that was even aware that this posed a problem.

There is significant public awareness of identity theft from other sources. We have all heard the stories of banks whose information gets hacked into by experts using computers and wireless routers; of individuals who rifle through dumpsters to find sensitive paper information that has been discarded; and e-mail addresses that get hacked into and information stolen. There are increasingly tight regulations about what information can be stored on computers. In the health-care industry, HIPAA has changed the way medical facilities do business. So there is considerable awareness of the problem, but until recently, no one was thinking much about what fertile ground the office copier/MFP provides for identity thieves. This situation has presented our industry with some challenges, but also some potential opportunities.

Virtually all digital copier/MFPs manufactured after 2002 have hard drives that store images of documents that are copied, scanned or e-mailed. The implications of this were brought to light earlier this year when CBS did a report centering on Dos Palos High School in Dos Palos, Calif. One of the CBS affiliate reporters pulled hundreds of students' names, home addresses, cell phone numbers and Social Security numbers from the hard drive of an old school copier/MFP. This reality caught the attention of the school superintendent, then Katie Couric of CBS and, ultimately, U.S. Rep. Ed Markey. Markey called for an investigation by the Federal Trade Commission, concerned that most



Americans do not know that their information can be compromised.

The publicity from the CBS report went further, with a reporter discovering (and reporting) that it is fairly easy to purchase used copier/MFPs that have been leased to businesses and are being resold in the United States or overseas and remove the hard drive that contains personal data. Many of these old copier/MFPs are available inexpensively enough so that this is an attractive option for those with ulterior motives.

While CBS may have been a bit overly dramatic with its “every-copier/MFP-holds-a-secret” storyline, it is nonetheless true. Consider for a moment what most businesses store on their copier/MFPs — paychecks, Social Security information, birth certificates, bank records, income tax forms, health-care records and much more.

When CBS reporters went to a warehouse in New Jersey to see how difficult it would be to buy a used copier/MFP loaded with information on the hard drive, they hit the jackpot. They were able to download sensitive police information, pay stubs, Social Security numbers and individual medical records.

So, that leaves us in the industry with some potential image problems and some hurdles to overcome. First, the perception is that the industry has failed in informing the general public of the potential risks involved with copier/MFPs. Our first challenge is to educate the public, and our customers, about the situation and what the industry (and we) can do to mitigate the problem.

To start, we need to find a way to assure the customer that data stored on the hard drives of the copier/MFPs they turn in as they come off lease is removed, or unavailable, to hackers. Several manufacturers have already taken steps in this direction. Konica Minolta has built-in protection on its equipment that overwrites data and then encrypts it. This can be set to be performed at certain intervals, or manually. Sharp has a similar solution in its Data Security Kit, which comes with a price tag of up to \$500.

The industry, in general, will need to move in this direction and manufacturers will need to have built-in and tested security devices that prevent data from being accessed. It may be

years in the future before it is uniformly done, so that means that there will be other issues to confront in the meantime.

Since we cannot return copier/MFPs to leasing companies without hard drives, we need to either assure customers that the data stored on these hard drives is secure, or factor into the sale or leasing price the replacement of the hard drive.

Certain industries, such as the banking and health-care industries, may have even more stringent standards they will expect the industry to adhere to. They are governed by Sarbanes-Oxley, HIPAA and Gramm-Leach-Bliley.

One banking transaction that we are aware of involves a multi-branch bank whose leases will soon be up for renewal. Because banks are already sensitive to identity theft, a solution for this institution is to have technicians on site at each branch location to remove the hard drives and hand them to bank officials, then substitute a new hard drive and return the copier/MFP to the leasing company. It solves the problem, but it is more costly.

Our industry needs to address this issue in a few key ways.

■ **Education** — It is incumbent upon dealers to communicate with customers about the potential for identity theft clearly and honestly. This can be accomplished through direct mail, PR, advertising, webinars or seminars. It is an ongoing process and educating customers about the potential threats is crucial. The education must go beyond what the industry is doing to deal with problems to secure confidential information; it should also alert customers to how they can establish security and safety protocols within their offices.

■ **Verification protocols** — Our industry needs to work out a way to have a standard, independent, dependable protocol

It is incumbent upon dealers to communicate with customers about the potential for identity theft clearly and honestly ... Educating customers ... is crucial.

for removing and overwriting data on hard drives. A standard system with benchmarks will help put this issue in perspective. Whether this ultimately results in replacement of hard drives and destruction of older ones, or simply overwriting, this needs to be a foolproof means of protecting data.

■ **Standardization of information protection** — It may be that all the inde-

pendent manufacturers will not immediately agree on how to protect information, but they should work toward that goal.

■ **Legislation** — With publicity and identification of a problem comes the likelihood that legislation will be introduced to address the problem. We should be open-minded to anything that protects our customers, the end users.

With problems come obligations and opportunities. We must do what we can to address the issue head-on to assure our customers that we, as an industry, are taking steps to protect them. For some, the manufacturer-provided solutions that primarily address end-of-lease issues may be sufficient. But for those who are more concerned with provisions of HIPAA and Sarbanes-Oxley, a more aggressive treatment may be in order. In those cases, they may seek our assistance in building an “overwrite-or-erase-as-you-go” program. We have the obligation to educate and the opportunity to provide products and service as needed. And, as this situation gets more and more attention, it may spur manufacturers to come up with newer and even better solutions. ■

Mike Arnold is president and CEO of CPO Ltd., Santa Clara, Calif. Visit www.cpoltd.com. For an additional perspective on the topic of security, see Peter Cybuck's article on page 18 in this issue.

