



Column Office Equipment, Inc
Distinctive Business Products, Inc.
Image Manufacturing, Inc.

Chicago Office Technology Group: 'Security is Not a Trend'

Hard drive removal and disposal service helps companies guard against potential data breaches

BOLINGBROOK, IL – May 10, 2010 – Periodically stories focusing on digital copier or multifunction product (MFP) security surface in the media. A recent CBS news story, 'Digital Photocopiers Loaded With Secrets,' warned of information theft risks associated with hard drives in digital devices. As many industry experts have been saying for years, copiers or MFPs are at risk for a data breach just like a laptop or a desktop PC.

"Security is not a trend for COTG. The security of our products and services has been a focus of ours since we started in the business," states Terry Dixon, President of COTG. "We have always been well-equipped to address any concerns that might be generated by stories of this type. Customers can have peace of mind knowing that with the manufacturers we represent, they have the most secure MFPs on the market."

All MFP devices COTG carries in the current product line-up meet strict data security standards as set by The Common Criteria (see www.commoncriteriaportal.org for more information). COTG carries the Xerox product line – Xerox is the only industry manufacturer to certify entire products, not only small components.

"Stories like CBS' are excellent reminders about how important it is to choose a vendor partner who will collaborate with you on a data protection strategy, not just sell you hardware," comments Ray Farias, IT Manager at COTG. "A solid strategy will include plans for end-of-life copiers or MFPs. One element of a solid end-of-life strategy is to actively remove any residual data. Residual data is what remains behind on a hard drive after any function - copy, print, scan or fax - has been completed."

COTG offers three options for data removal on the hard drive before the MFP is disposed of or turned in after a lease:

1. The hard drive is 'shredded' using an industrial data destruction machine. COTG will furnish a certified document as proof of destruction.
2. On-demand electronic erasure of the hard drive, which follows a security process originally developed by the U.S. Department of Defense. COTG will also furnish a certified document as proof of data removal.
3. A certified technician will remove the hard drive and return it directly to the customer for disposal. The technician will educate the customer about potential security risks and the features available to address them.

Companies can feel confident knowing the right MFP-based security tools and policies are in place when purchasing devices from COTG. Many of the features listed below come standard with Xerox devices or are available as options:

1. **Image Overwrite:** Electronically 'shred' information stored on the hard drive of MFPs. Electronic erasure can be performed automatically at job completion or on demand.
2. **Secure Access Unified ID System:** Integrates your MFP with your existing employee ID badge solution to provide a flexible authentication system. Users simply swipe their magnetic ID card for secure access to MFP functions that need to be tracked for accounting or regulatory requirements.
3. **Embedded Fax:** While firewalls work at the network periphery to prevent unauthorized access to a customer's environment, unprotected fax connections in MFP devices can be an open "back door" into the network. We assure complete separation of the fax line and the network connection.

Proven Leadership. Powerful Results.

4. **Access Controls and Usage Audits:** Requires authorization in order for people to use the walk-up copy features of the device. Administrators can also limit the number of copies available for each user, track usage at an account or department level and download data to generate audit reports.
5. **Network Authentication and Authorization:** Access to scan, email and fax features is restricted by validating network user names and passwords prior to use of these functions. All activity is monitored and recorded in a security audit log.
6. **Removable Disk Drive Accessory:** Administrators can physically remove hard drives, virtually eliminating the risk of unauthorized access to classified data.
7. **Secure Print:** Jobs are safely stored at the device until the owner enters a PIN to release them. This controls unauthorized viewing of documents sent to the printer.
8. **Encryption:** All data moving in and out of the device, as well as data stored within the device is secured with state-of-the-art encryption.

For more information about hard drive removal and disposal as well as standard and optional security features on your copier or MFP, please contact your sales representative.

About Chicago Office Technology Group

We are Chicago's largest technology and services company specializing in workflow solutions and office systems. From document management to collaborative communication tools and multifunction systems, we provide the broadest portfolio of technology and services for companies of any size and in any industry. We focus on document-driven companies and industries - from healthcare organizations, manufacturing companies and legal firms to school districts and financial service institutions - spanning all types and sizes. To bring comprehensive solutions to the market, we partner with world-class innovators and value-added suppliers.

We operate with branch offices in Chicago, Itasca, Tinley Park and Bolingbrook, Illinois as well as Minneapolis, Minnesota.

XXX

For further information please contact us at 800-895-2585 or visit our website at www.cotg.com. Find us on Facebook and LinkedIn – keyword 'Chicago Office Technology Group'