Randall R. Cusick
Manager, Technical Marketing
XNA Marketing Operations

April 20, 2010

Re: Digital Photocopiers Loaded With Secrets - CBS News Story

Periodically stories focusing on digital copier or multifunctional product security surface in the media.

Xerox has been at the forefront of the digital copier product security movement that began in January 2000, when the Federal Government released an instruction called NTISSP 11. This instruction required agencies of the Federal Government insure the secure functioning of network-connected devices, even those that fell into the COTS (commercial, off-the-shelf) classification.

An element of secure functionality is to actively remove any residual data. Residual data is what remains behind in electronic memory or on disk drives after any function (copy, print, scan, fax) has been completed. Xerox addressed that requirement first in 2001 with an optional feature called 'Disk Image Overwrite' that would 'scrub' the disk drives in accordance with US Department of Defense specifications, the most stringent requirement at that time. That capability moved through most of our product portfolio after 2001, and now is available in nearly every disk equipped product Xerox offers.

At the end of 2006 Xerox made the decision to include the Disk Image Overwrite option as a standard feature on most of the products in the Office portfolio, and to allow installation of the option at no charge on the products in customer sites that previously offered the option for a fee.

At the same time, Xerox also instituted a program allowing customers to purchase disk drives, at an attractive price, from any Xerox product at the end of lease or product removal. The purpose of this program is two-fold: to allow very high-security locations positive control of the disk drive, and to provide a secure solution for earlier products that did not offer a Disk Image Overwrite capability.

Randall R. Cusick
Manager, Technical Marketing
XNA Marketing Operations

Selected Xerox products are submitted for an exhaustive security testing and certification process, known as "The Common Criteria for Information Technology Security Evaluation", or, in shorthand, "The Common Criteria". The Common Criteria Mutual Recognition Arrangement is comprised of 26 member nations that test and certify information technology products to common security guidelines.

Xerox has enjoyed a competitive advantage for several years as the only MFP vendor to certify the entire product, including all components and functions. Other vendors have certified only small parts of their products, leaving untested potential vulnerabilities. See www.commoncriteriaportal.org for more information.

We have an active and informational security component of our public-facing web presence. Guidance is offered on this site for secure operation of Xerox products. See www.xerox.com/security

There is also a very active security-focused community of practice inside Xerox addressing not just our product security, but security of our transactional business and that of the Xerox infrastructure.

In summary, Xerox is very well equipped to address any concerns that might be generated by stories of this type, and has enjoyed a leadership role in product security for the last 8 years or so. We are striving to keep that leadership position.

Best Regards,

R. Cusick

Randall R. Cusick

Xerox Corporation
8823 Fort Drive
Manassas, VA 20110-4966
Telephone 703.335.7426
Facsimile 866.588.8974