

A Document Security Handbook

**Are you sure your
confidential documents
are as secure as they
need to be?**

**Creating secure document management processes
and protecting document confidentiality.**

Prepared by Xerox Corporation

THE DOCUMENT COMPANY
XEROX[®]

A heightened mandate for security in anxious times.

Protecting sensitive, proprietary or classified information has always been challenging. Nevertheless, before the advent of today's digitally networked offices and increasingly sophisticated threats, maintaining airtight security of confidential documents often meant simply putting those documents away and locking the door behind you at the end of the workday.

In this uneasy, post-9/11 environment, however, managers in government as well as healthcare, financial services, pharmaceuticals and other segments of corporate America are more aware than ever before of the need for deploying more sophisticated document security processes and technologies to ensure confidentiality.

What's driving the increased attention to security?

Threats to information security come from both internal and external sources. They can be online or local and range from accidental to malicious to criminal attacks by hackers, disgruntled employees or even spies.

In addition to these new threats, the growing complexity of office products, services and systems has become a contributing factor to the heightened risk of document security incursions. Offices have become highly interactive environments of powerful multi-function devices and interconnected systems across global networks. The introduction and proliferation of digital and networked copiers, printers and multifunction devices

into this milieu has created new sets of document security vulnerabilities and new windows of opportunity for those who wish to exploit them.

Regardless of who illegitimately accesses your systems, they have numerous means by which they can expose your most sensitive business information to unauthorized use, disclosure, modification or total loss. This underlies the need for greater comprehension of a wider variety of processes, systems and technologies in order to instill confidence in the overall security of any enterprise IT system.

The more ways into a system, the more ways for information to leak out.

The ultimate strength of an overall information assurance strategy depends upon creating an impenetrable chain of security links, including people, processes, work procedures, and the systems and technologies that support them all. A weak link anywhere in this chain presents a security risk.

Yet while most organizations have comprehended overall network security into their information assurance strategy, the most common document output processes—printing, copying, scanning and faxing—often are an innocently overlooked area which, if not comprehensively accounted for, can create security vulnerabilities within the organization's information security chain.

What are some of the ways that document security can be breached?

- Every time a copy or print job is performed on a digital copier or printer, a remnant of the image is stored on the device's hard disk drive and network controller disk. These document artifacts can be pilfered from the hard disk drives via either electronic or physical access.
- Documents lying on a copier or printer output tray can be stolen, viewed or copied by unauthorized persons, while the "owner" who originated the print job walks to retrieve the sensitive output.
- Persons can obtain unauthorized network access, or invoke unauthorized user privileges, to gain access to sensitive documents that are not protected within a secured document management system.
- Confidential hard-copy documentation can be scanned directly to external e-mail distribution by individuals not authorized for such rights. In addition, many systems have no ability to track such unauthorized usage; thus, once the hard copy is put back in its original place, it is extremely difficult to track the transmission to the perpetrator.
- Malicious vendor service technicians can gain access to critical documentation via any one of the above-mentioned means.

U.S. policy directive leads the way toward more comprehensive security assurance strategies.

In recent years the U.S. government has begun migrating from the exclusive use of Government Off-the-Shelf (GOTS) products to include more Commercial Off-the-Shelf (COTS) products for the protection of our national security systems.

As a result of that migration, it has become critical for users of those systems to have a means to validate that information assurance (IA) products provide the advertised security functionality.

Meeting the National security challenge.

National Security Telecommunications and Information Systems Security Policy No. 11 requires that information assurance standards be applied to all systems used to enter, process, store, display or transmit national security information.

Specifically, only IA and IA-enabled IT products certified by the NIST FIPS or the National Information Assurance Partnership (NIAP) may be acquired by government agencies working with national security information. The standard of certification, known as the Common Criteria (ISO 15408), has been adopted by 14 nations and is recognized worldwide as the primary measurement for IT security.

NSTISS Policy #11 leads the way for coherent deployment of information assurance systems.

Besides federal government agencies, which are now mandated by law to adhere to Policy 11 recommendations, organizations within the non-federal public sector as well as the private sector are beginning to follow the federal government lead and integrate similar purchasing guidelines for IT systems.

Creating an airtight document security environment.

According to NIAP, links in the security chain include access control mechanisms, identification and authentication devices, audit mechanisms, encryption mechanisms, firewalls, smart cards and biometrics.

With all these components, it is no wonder that NIAP says the choice of products significantly affects the security of systems in the critical information infrastructure and its office equipment.

For many organizations within government, doing business with the government, or seeking the ultimate standard in document security, the product of choice is a Xerox Document Centre® system.

The industry's first truly secure networked digital multifunction systems.

Xerox Document Centre systems with Image Overwrite Security are the only networked digital multifunction systems currently under evaluation by NIAP for security certification at Common Criteria Evaluation Assurance Level 3 (EAL3).

Xerox is obtaining Common Criteria Certification for the Document Centre 490/480/470/460 Network Multifunction System Controller and corresponding security software.

Image Overwrite Security: the linchpin capability for unbreakable protection.

Every time you print, copy, scan or fax sensitive information, an image of it is stored on your digital copier or printer hard disk drive. You could have a serious security breach on your hands if those disk drives are ever stolen or misplaced.

The Image Overwrite Security option provides the capability to overwrite residual user document image data remaining on hard disks after a print, copy, scan or fax operation.

- As its name indicates, Image Overwrite Security actually clears or “overwrites” all trace of any image captured on your copier hard drive by using a three-pass process specified by the U.S. Department of Defense.
- Because images are also stored on your network controller hard drive whenever you print from the network, Image Overwrite Security writes over these, as well.

These features make Xerox Document Centre products with Image Overwrite Security the most secure networked multifunction systems on the market today.

The Xerox Document Centre® — multiple security features deliver unparalleled protection throughout the document lifecycle.

Other Document Centre Security Features:

Removable Disk Drive Accessory—Enables the physical removal and secure storage of Document Centre hard disk drives. When combined with Image Overwrite Security, it guarantees comprehensive assurance against document disk drive image latency for the most demanding security requirements.

Secure Print—Allows print jobs to be sent, and held in the print queue until the creator enters a unique PIN (personal identification number) at the output device. This eliminates the risk of confidential documents printing lying unattended in the document output tray, where they are vulnerable to theft and unauthorized viewing.

DocuShare—A Web-based document management system providing a comprehensive solution for the most complex document archiving and access requirements. It allows you to create multi-tiered levels of authority for various groups of individuals to retrieve, view, edit, manage and output documents within a highly organized archival system. You can totally restrict access to certain documents and folders, thus ensuring confidentiality and user privileges across Internet and intranet applications.

E-mail, Scanning and Network Fax Authentication—A robust set of tools enabling Network Administrators and other authorized individuals to restrict and control access to Document Centre e-mail, network scanning and network faxing functionality. In addition to access rights, the system requires entry of a user login/password to ensure user authentication and accountability, and tracking of all activities.

Information is every organization's most important asset.

Very little question remains about whether or not a business needs a document security strategy. Xerox Document Centre systems, with built-in security features and options such as Image Overwrite Security, are designed to minimize your exposure and manage risk. In the face of today's security challenges, the real question is, how quickly can your security program be up and running?

**For more information about
Image Overwrite Security for
Xerox Document Centre systems,
call 1-800 ASK-XEROX, ext. SAFE.**

© 2002 XEROX CORPORATION. XEROX®, The Document Company®, Document Centre®, and all Xerox products mentioned in this document are trademarks of or licensed to XEROX CORPORATION. All rights reserved.