

Xerox Security Summit Fact Sheet

Security is a major concern for enterprises of all sizes. Driven to keep ahead of the growing number of threats facing organizations today, Xerox has emerged as a leader in protecting intellectual property and anticipating what's next in the world of document security. One of the leading vulnerabilities to a corporation is the unprotected documents within the organization. With the growing concern that proprietary information in the wrong hands can be a threat to not only the corporation, but also to national security, Xerox assists companies arm themselves with products and services to protect, manage and distribute information.

Industry Stats on Security

- Documents - on desktops and in filing cabinets, in personal emails and databases - contribute to 80 percent of every security breach, according to a study by the Computer Security Institute and the FBI.
- According to Xerox, 80 percent of corporate espionage occurs through documents.
- Xerox estimates that large enterprises create more than 850 million impressions of their data per year using printers and copiers, leaving large amounts of data vulnerable.
- Unauthorized access is the second most significant contributor to computer crime losses, accounting for 24 percent of overall reported losses, showing a significant increase in average dollar loss from the previous year. (Source: 2005 Computer Security Institute/FBI Survey)
- According to Xerox, the average age of devices, including printers, copiers, fax machines, multifunction devices and scanners within corporations today is six-to-eight years old. Devices this old predate critical regulation, like Sarbanes-Oxley and Gramm-Leach-Bliley, and therefore don't meet the necessary security requirements.
- According to the 2005 Computer Security Institute/FBI Survey, the average loss due to the theft of proprietary information more than doubled between 2004 and 2005.

Xerox Security Fast Facts

- Xerox has five research centers worldwide spending six percent of its annual revenue on security and other critical research, development and engineering projects.
- Xerox products are designed to support standards set forth in The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Gramm-Leach-Bliley Act and FDA 21 CFR Part 11.

Common Criteria Certification Fast Facts

The threat of data loss and non-compliance penalties makes it essential that companies have a plan to secure their networked peripherals. The National Information Assurance Partnership (NIAP) is a U.S. government initiative designed to meet the security testing needs of both information technology manufacturers and users, and the Common Criteria Certification program is an internationally recognized standard for security claims of IT products and systems.

- Xerox has earned Common Criteria Certification on 30 of its multifunction systems.
- To achieve the Common Criteria Certification, manufacturers must secure the device's hard drive. Xerox goes beyond that by further securing all eight points of entry on its devices. They are the only manufacturer to do so. Xerox is also the only manufacturer that assures complete separation of the telephone line and network fax connection. While firewalls prevent unauthorized access to a customer's system through the network connection, unprotected fax connections in multifunction devices can be an open back door to the network.
- The U.S. Department of Defense requires all IT products used within the department, all military branches, and buildings such as the Pentagon to have Common Criteria Certification.

For information on Common Criteria Certification and Xerox-certified products visit: www.xerox.com/security.

Specific Xerox Security Solutions

- **Device Access Password Protection** - Administrative device set-up screens and remote network settings cannot be viewed or altered without a PIN.
- **Configurable Network Services** - Secures networked devices by allowing enablement/disablement of specific device and print protocols.
- **Removable Disk Drive Accessory** - Lets users remove and store hard drives, virtually eliminating the risk of unauthorized access to classified data.
- **Network Authentication** - Restricts access to scan, e-mail, and fax features by validating network user names and passwords prior to use of these features.
- **Omtool's Genidocs** - A Xerox Premier Business Partner solution, available on WorkCentre Pros, addresses regulatory compliance and privacy protection. Encrypts outbound documents, decrypts them upon receipt, enabling compliance with government regulations.
- **Internal Auditron** - Prevents unauthorized users from using walk-up copy features. Number of copies available for each user can be limited by tracking usage to an account or department.
- **Secure Embedded Fax** - Prevents unauthorized control of the device via the fax subsystem. Faxes can be automatically routed to a password-protected fax mailbox or stored at the device until an authorized user releases them for printing.
- **Categorizer** - Powerful software that can "read" an electronic document, decide how it should be classified by subject and then automatically route it to the right person's e-mail address or to an online document management system.
- **ContentGuard Software** - Allows companies to track who accesses what information on their Web site, providing protection of digital content.
- **DataGlyph** - A two-dimensional symbology for encoding machine-readable data onto paper documents or other media. DataGlyph technology allows documents to carry thousands of characters of information hidden in gray patterns that can appear as backgrounds.
- **Image Overwrite Security** - Enables organizations to overwrite images captured on both the network controller hard disk drive and the main disk drive of a Xerox networked copier or multifunction device.
- **SecurePrint** - Holds jobs at the device until the owner enters a PIN to release them.