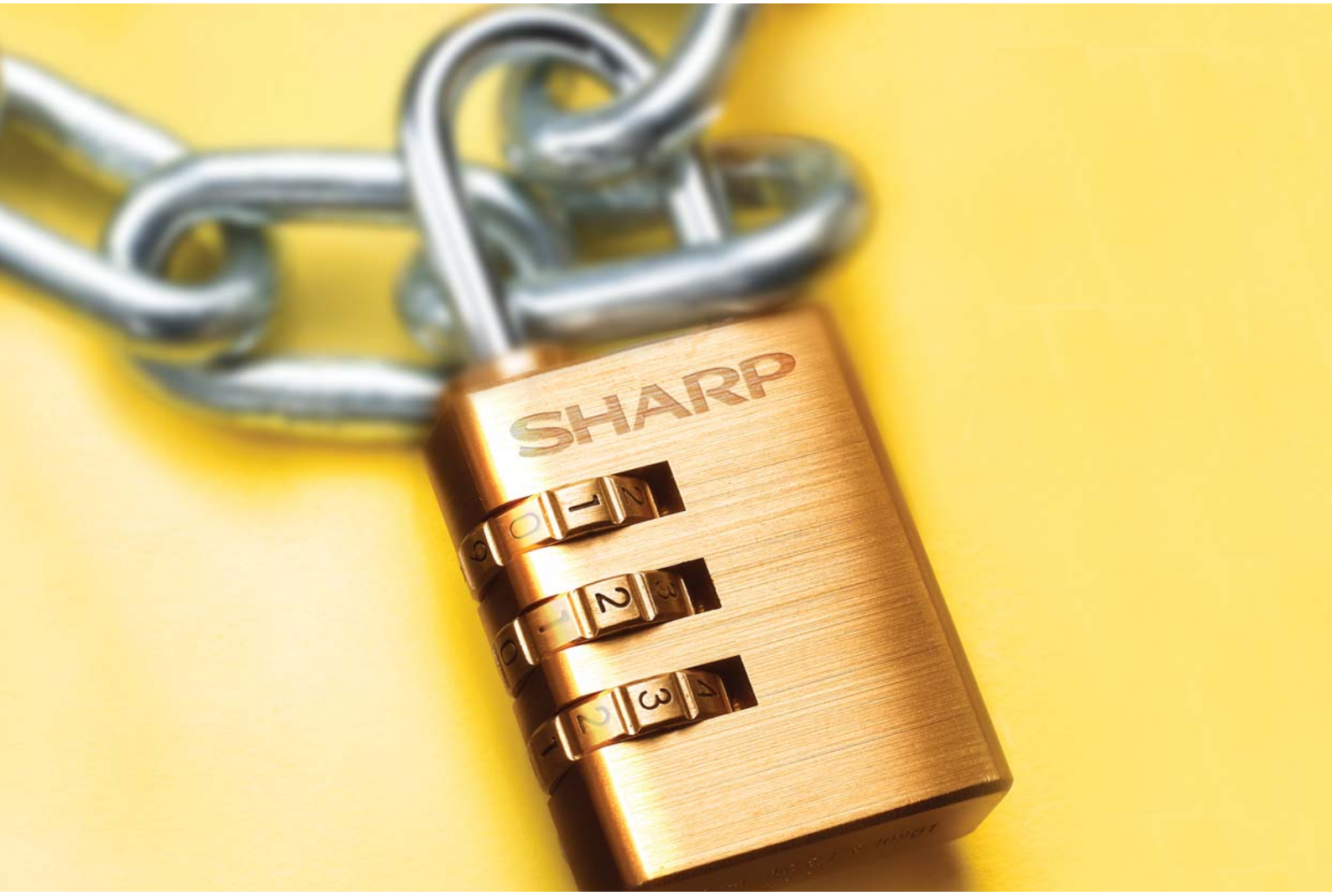
SHARP

DOCUMENT SECURITY SOLUTIONS



PROVEN SOLUTIONS FOR TIGHTER NETWORK SECURITY

SHARP ***DOCUMENT*** SOLUTIONS

COMMON WEAKNESSES IN NETW

Poor network security can lead to loss of intellectual property, lack of credibility with your investors and partners, problems with data protection legislation, poor morale in the workplace, and more.

Like most companies, you protect your network with firewalls. You defend against trojans and worms. And you probably use encryption. But unless you've secured your network printers, copiers and multifunction peripherals (MFPs) from attack and misuse you're still at risk.

ORK SECURITY...

THREAT 1

Digital printers, copiers and multifunction devices have hard disks that still retain hundreds of pages of confidential data long after the document was created.

THREAT 2

A hacker can gain enough information from viewing the configuration settings of a printer's network interface card to launch a major attack on your network.

THREAT 3

Information sent across a network to a printer or MFP is vulnerable to interception.

THREAT 4

Copiers and MFPs provide a quick, untraceable means of copying and electronically distributing sensitive documents.

THREAT 5

MFPs with unrestricted or unmonitored access can be used to anonymously copy and/or electronically distribute sensitive information.

THREAT 6

Documents sent in unencrypted emails by MFP's can be vulnerable to interception and/or incorrect delivery.

...AND HOW TO FIX THEM FOREV

DATA SECURITY KIT

Without proper protection, the hard disks in your printers, copiers and MFPs pose an unacceptable security risk. And that's why we developed our Data Security Kit - the industry's first Common Criteria validated solution for document and information security.

> ***Common Criteria explained***
>
> *Common Criteria is the emerging standard for IT security testing (ISO 15408) and an internationally recognised methodology for evaluating the security claims of information systems, hardware, and software vendors. These standardised evaluations validate the accuracy of the claims of the product, providing users in security-conscious environments with increased confidence and peace of mind.*

Featuring a dependable combination of secure erasure and data encryption, Sharp's Data Security Kit makes it virtually impossible to intercept or recover data that's left behind on your printer or copier.

Data Encryption

128-bit data encryption for printers and copiers – another first from Sharp

Encryption technology is widely used to protect all sorts of data. But, until now, it's been conspicuously absent from printers, copiers and multifunction devices, creating a known but widely ignored security vulnerability.

At Sharp, we believe in protecting your data from the second it's created to the moment it's discarded.

The Data Security Kit applies a powerful 128-bit data encryption algorithm to the data as it is written to the internal hard drive, RAM and ROM. That means that even if someone did manage to access to your printer or copier, any retrieved data would be unintelligible and therefore useless.

Common Criteria Validated

MFP Data Security Kit
MX-FRX1 version M.10

ER

Data Overwrite

The Data Security Kit's secure overwrite feature adds even more security by 'shredding' residual data on the hard disk, ROM and RAM. Now you can securely erase left over files by overwriting them up to seven times with a series of random values. Coupled with our unique encryption protection, the Data Overwrite feature completely prevents the recovery of residual data by any commercially available means.

For added convenience, the Data Security Kit can be configured to overwrite the data in one or more of three ways:

- Automatically, each time the device is powered up
- Automatically, after each print/copy/fax/scan operation
- Manually, on-demand

Confidential Print Function

Our Confidential Print Function adds even more security by requiring the user to be present at the machine before the document is produced. Print runs are initiated in the normal way but output is delayed until the originator personally enters a PIN code on the front panel of the printer: a practice that eliminates the risk of confidential documents being left out in the open.

at a glance...

- *Encrypts hard disk data*
- *Hard disk data erased/overwritten after copy, scan, fax and print use*
- *Runs automatically without user intervention*
- *Tamper resistant*
- *Supports PCL5, PCL6 and Postscript*
- *Common Criteria accredited to ISO 15408*

SECURE NETWORK INTERFACE

Network Interfaces also pose a security risk. A determined hacker can gather enough information to prepare a serious attack on your main network servers, just from viewing the configuration settings of an unsecured Network Interface.

Sharp's Secure Network Interface provides a firewall to each printer or copier, preventing unauthorised access to configuration details and network settings, and restricting usage to identified print servers and specific users. This eliminates the risk of external attacks without compromising the needs of the users or the remote access abilities of the system administrator. Access can be controlled at 3 levels:

- **IP address filtering**, which limits access to a select number of pre-defined addresses
- **MAC address filtering**, which limits access to specific PC's regardless of their IP addresses
- **TCP/IP services blocking**, which block specific communications protocols and gives administrators the ability to close vulnerable ports and disable the embedded home page of the device.

Sharp MFP Network Security compatibility IP address/MAC address filtering
Access filtering is controlled on a secure area of the configuration web page of the MFP device.

Access to and from the MFP can be limited to designated IP addresses or address ranges. This means that in a small peer to peer network environment access is restricted to an identified workgroup.

MAC address filtering is a much tougher filter, since a MAC address is unique to a network card. MAC address filtering is recommended when a device is connected to a greater enterprise network, where IP addresses can be reconfigured to steal identity. Typically a Print server MAC address will be permitted, with a backup address for an administrator. All other users will only have access through the print server. For desktop scanner usage, additional MAC addresses may be necessary.

Up to 4 IP address ranges can be defined, and up to 10 MAC addresses can be designated. IP address filtering can allow or deny transmission to designated IP addresses (MAC address filtering can only allow transmission).

Protocol filtering

Network connection and conformity to standards such as TCP/IP introduces many "back door" methods of communication that are not well publicised, but understood by programmers and network specialists.

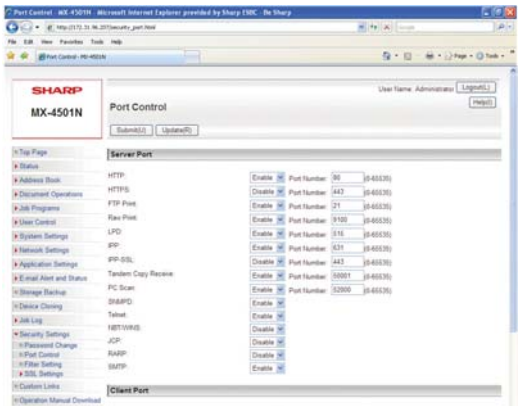
Sharp MFP network interfaces offer the ability to block these protocols, and change default port settings for Internet access.

Reasons for filtering ports and access:

- **Blocking of Telnet:** Prevents administrator password from being seen as plain text.
- **Blocking of RARP:** Prevents malicious RARP server from assigning IP address without permission.
- **Blocking of JCP:** Prevents administrator password from being seen as plain text.

More recently, additional control and filtering has been added to block SNMP protocol, and to change the HTTP port access number (commonly known default is 80).

Protocol filtering is controlled on secure areas of the configuration web page of the MFP device.



SSL (SECURE SOCKETS LAYER)

As data is sent to an MFP – either by way of a document that is to be printed or as an exchange of information between the device and the system administrator – it has the potential to be intercepted by a third party.

SSL encrypts the information in the data stream from the moment it is sent to the moment it is received by the MFP. As well as protecting documents that are being sent to print, this feature also encrypts any information exchanged between the MFP and the administrator, who can view the MFP's internal web page in a secure mode (HTTPS). The level of encryption can be set as low, medium or high.

This feature also makes use of digital certificates to uniquely identify the MFP across the network, even if the IP address has been changed.

benefits at a glance...

- *Prevents information that is sent to the MFP from being intercepted and retrieved.*
- *Lets you securely print documents from anywhere on the network.*
- *Allows administrators to securely view the MFP's internal web page from any location on the network.*
- *Provides positive proof of the MFP's identity across the network.*

DOCUMENT CONTROL

Modern MFPs can copy multi-page documents in a matter of moments. And many of them have the ability to send copies by fax or email to anyone, anywhere in the world. But what if the document is strictly confidential and was never meant to be copied? That's when you need Sharp's Document Control feature.

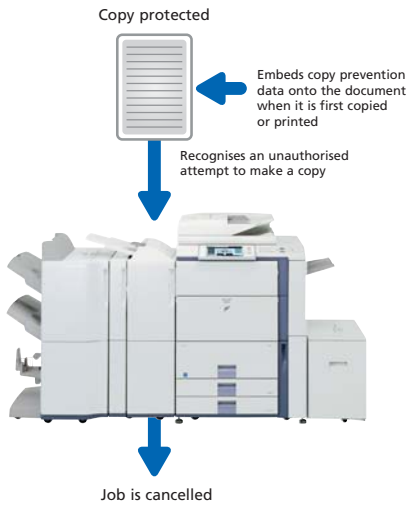
Document Control*1 works by embedding copy prevention data onto hard copy documents as they are created by the MFP. This data, which appears on each page as a barely visible pattern, prevents a document from subsequently being copied, scanned, faxed or filed. Any unauthorised attempts to copy a Document Controlled-document will simply be cancelled*2. The MFP will also generate an e-mail alert to notify the administrator.

Document Control is available on the MX series of colour MFPs that have been equipped with the Data Security Kit.

benefits at a glance...

- *Prevents unauthorised copying, scanning, faxing and filing of sensitive documents.*
- *Does not significantly alter the appearance of the original document.*

Document Control Function



*1 Requires optional Data Security Kit. May not work for certain types of documents and paper.

*2 May result in the output of a blank page if paper has already been fed for the job before the MFP detects copy prevention data.

INTERNAL USAGE AUDITOR AND USER AUTHENTICATION

Network-connected MFPs can scan documents and distribute them across the Internet to virtually anywhere in the world. This ability, plus the tendency to situate MFPs where they can be accessed by the greatest number of people, creates a potential opportunity for data theft. Sharp's Internal Usage Auditor and User Authentication features eliminate this threat by letting you control, monitor and record who uses your MFPs.

Internal Usage Auditor

Internal Usage Auditor lets you control local access to the MFP, by requiring users to enter a personal 5 digit code at the start of the job. Once the job has been completed, details about how many pages were produced and by whom are accumulated into an internal accounting log for later collection. The account information can also be emailed to a central collection point.

User Authentication

User Authentication adds a top level of security and protects valuable network resources by limiting access to registered users with valid network accounts. Before starting a scan, the user must first enter a username and password which are authenticated against the global address book on a designated server.

For added convenience and traceability, the operator's email address is added to the "from" field of the sent document, and a blind copy can be sent to your network administrator, or to an archive to keep a record of all scanned documents. A log is kept for an audit trail of document scans.

benefits at a glance...

- *Eliminate the security risks presented by a network-connected MFP.*
- *Provides a detailed record of who has used the MFP, when and for what purpose.*
- *Prevents operation by unknown or unauthorised users.*
- *Prevents scanned documents from being emailed to unknown addresses.*

Sharp MFPs offer up to 5 different levels of Authentication method: Anonymous, Simple, Digest MD-5, NTLM and Kerberos.

For more controlled destination management, Sharp MFPs interface directly to Lightweight Directory Access Protocol (LDAP), so that all send destinations can be setup and maintained on a central server, thus preventing illegal destinations from being locally configured on the MFP.

ENCRYPTED PDF

The ability of MFPs to scan documents and send them as PDF files to local or remote destinations via email creates the potential risk of either accidental or deliberate interception by an unauthorised person. So if the nature of your work means that you deal with confidential information encryption is a sensible precaution.

Suitable for scanning to e-mail, FTP, Desktop, HDD and USB, Sharp's Encrypted PDF function uses RSA technology to encrypt the file before it is sent. The user is prompted to create a password at the time of scanning and the recipient can only view the file if he or she knows the correct password. Encrypted PDF is available as an option on the MX series of colour MFPs.

benefits at a glance...

- *Encrypted PDF protects scanned documents with password controlled encryption.*
- *Prevents unauthorised printing or viewing of documents that have been scanned to a PDF format and sent to email, FTP, Desktop, HDD or USB.*

SECURITY FEATURES OVERVIEW

Product Feature		BLACK AND WHITE					COLOUR		
		AR-M150 AR-M155	AR-M165 AR-M207	AR-M256 AR-M316	MX-M350 MX-M450	MX-M550 MX-M620 MX-M700	MX-1800N MX-2300N MX-2700N	MX-3500/01N MX-4500/01N	MX-5500N MX-6200N MX-7000N
Data Security Kit *[1] - Option				AR-FR24U*[2] AR-FR25U*[3]	MX-FRX6U*[4] MX-FRX7U*[5]	MX-FRX5U	MX-FRX1	MX-FRX2	MX-FRX3
	Hard Disk Erase by overwrite			N/A	✓	✓	✓	✓	✓
	All Memory erase by overwrite			✓	✓	✓	✓	✓	✓
	Number of times of overwrite			1	1 to 7	1 to 7	1 to 7	1 to 7	1 to 7
	AES Data Encryption on HDD			N/A	✓	✓	✓	✓	✓
	AES Data Encryption on RAM memory			N/A	✓	✓	✓	✓	✓
	AES Data Encryption on Fax memory			✓	✓	✓	✓	✓	✓
Network Firewall	IP Address Firewall	✓	✓	✓	✓	✓	✓	✓	✓
	Mac Address Firewall	✓	✓	✓	✓	✓	✓	✓	✓
	Protocol and port service access control	✓	✓	✓	✓	✓	✓	✓	✓
User Access control		✓	✓	✓	✓	✓	✓	✓	✓
Configuration Access control		✓	✓	✓	✓	✓	✓	✓	✓
Confidential PIN Print Function				✓	✓	✓	✓	✓	✓
External Secure Print Release - Option		✓	✓	✓	✓	✓	✓	✓	✓
Warning message 'Original still on scanner'			✓	✓	✓	✓	✓	✓	✓
Internal Usage	Print		✓	✓	✓	✓	✓	✓	✓
Auditor	Copy	✓	✓	✓	✓	✓	✓	✓	✓
	Fax		✓	✓	✓	✓	✓	✓	✓
	Scan		✓	✓	✓	✓	✓	✓	✓
LDAP address book access control*[6]		✓	✓	✓	✓	✓	✓	✓	✓
Sender email authentication*[6]				✓	✓	✓	✓	✓	✓
Sender email audit trail*[6]				✓	✓	✓	✓	✓	✓
SSL (Secure Sockets Layer)				✓	✓	✓	✓	✓	✓
Encrypted PDF							✓	✓	✓
Document Control - Option (requires Data Security Kit)							✓	✓	✓

*[1] Check local availability

*[2] For AR-M256 *[3] AR-M316 *[4] For N model *[5] For U model

*[6] Full details provided in Advanced Image Distribution brochure

SHARP

Design and specifications are subject to change without prior notice. All information was correct at time of print. Windows and Windows NT are registered trademarks of Microsoft Corporation. All other company names, product names and logotypes are trademarks or registered trademarks of their respective owners. © Sharp Corporation 2007 Ref. Security_June07 All trademarks acknowledged. E&OE.