DIGITAL DOCUMENT SYSTEMS GROUP

SHARP

Document Security

Understanding and minimizing the risks

Peter Plested

Sharp Electronics Europe

Data Security

- Understanding the risk
- Encrypting data and erasing data
- IP/MAC Address Filtering
- Confidential Print
- Network User Authentication
- Copy Prevention
- Network data encryption

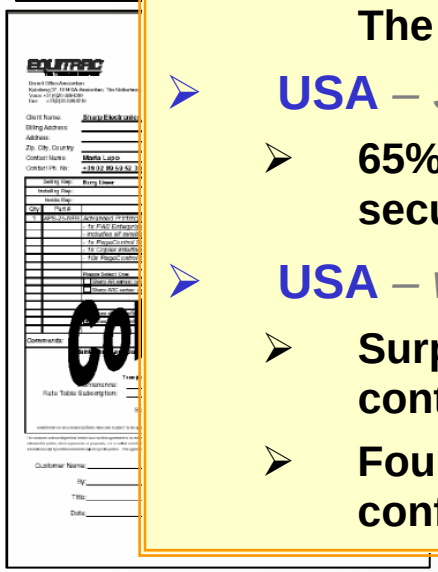
DATA SECURITY

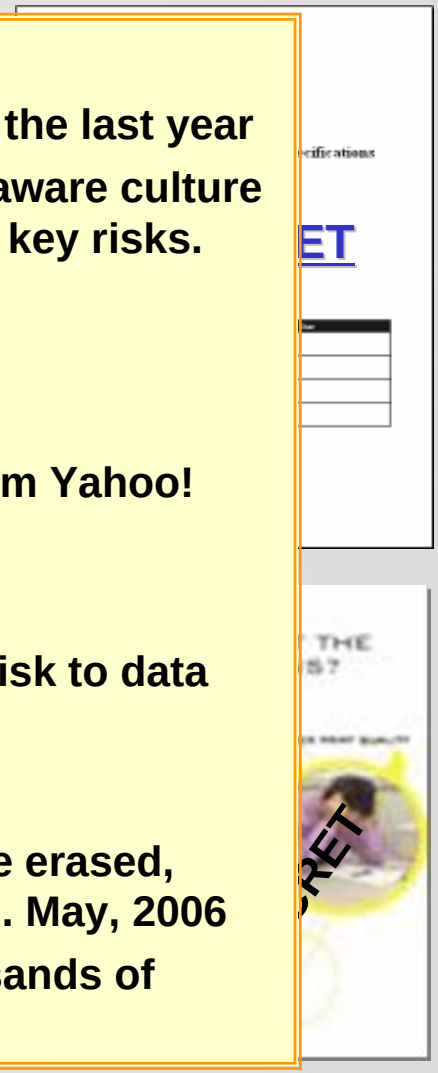
- Organisations such as Government, Military, finance, and legal, have long been concerned about information security.
- With the expansion of IT availability we now find commercial organisations are also demanding higher IT security when purchasing IT related products.
- However in most of these cases, the Management and staff have little or no idea that digital MFPs and Printers present a security risk.
- While this risk, might pose commercial and national security concerns there is also potentially an unforeseen breach in Data Protection compliance acts

SHARP

AWARENESS OF DATA SECURITY IS ON THE INCREASE

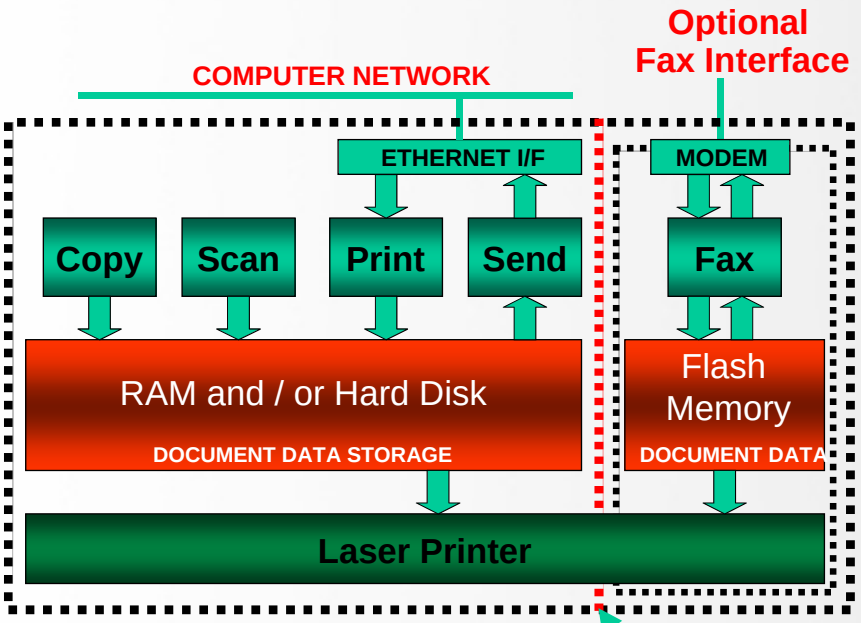
- **UK** - *DTI Information Security Breaches survey 2006*
  - **62% of UK companies had some form of security incident in the last year**
  - **Many UK businesses are a long way from having a security aware culture Their expenditure on security is either low or not targeted at key risks.**
  - **The average cost of a worse case security incident :- £12,000 (small businesses) , £90,000 (large businesses)**
- **Japan** - *News article, Feb. 24, 2004*
  - **The personal information of 4.5 Million people leaked out from Yahoo! The total compensation amount was approx €20Million.**
- **USA** – *Sharp commissioned survey of 1100 IT professionals*
  - **65% of IT professionals thought that a copier presented no risk to data security.**
- **USA** – *www.privacyrights.org/ar/ChronDataBreaches.htm*
  - **Surplus government computers sold before hard drives were erased, containing credit card numbers and social security numbers. May, 2006**
  - **Four hard drives sold on eBay containing hundreds of thousands of confidential company documents and records. May, 2006**





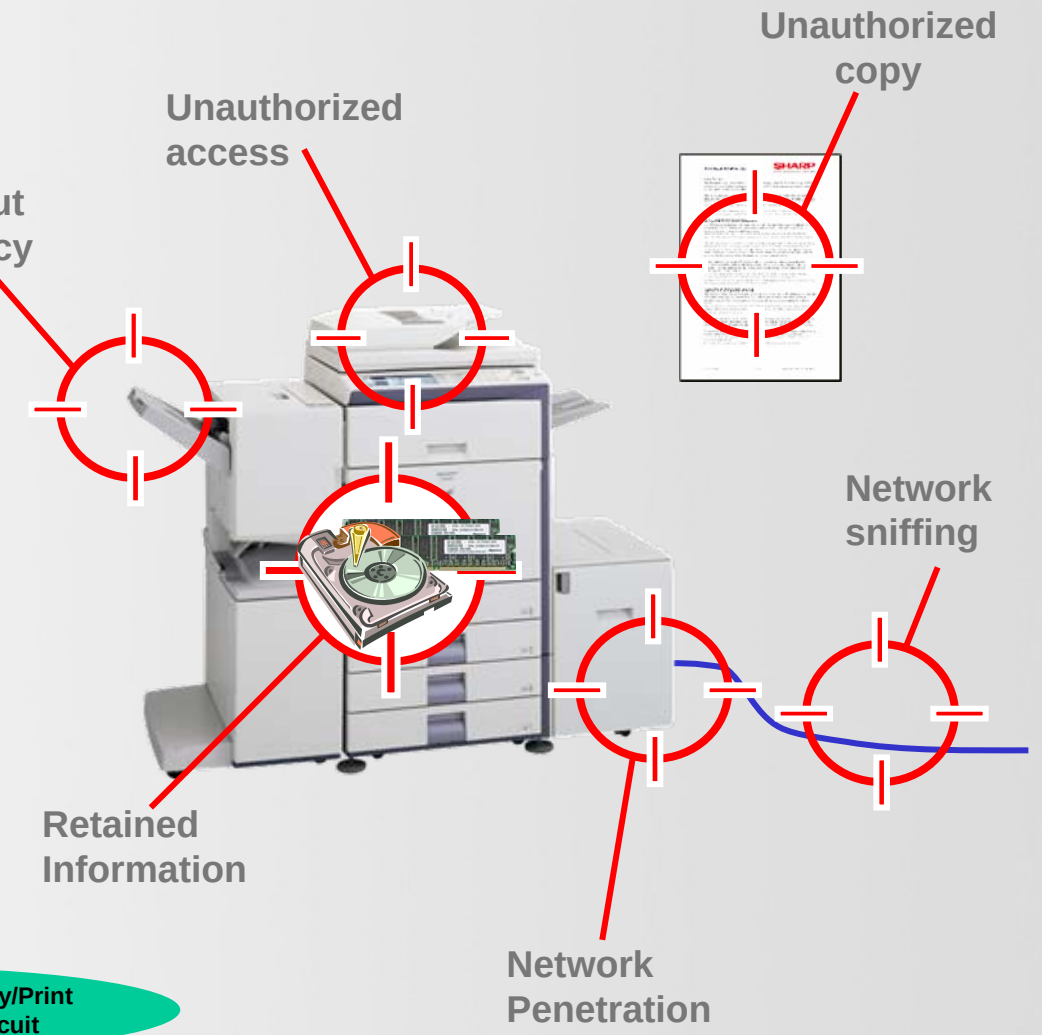
UNDERSTANDING THE RISK…

Points of vulnerability



MFP Architecture

Isolation of Network and Copy/Print Data from Fax Modem Circuit



UNDERSTANDING THE RISK…

example.swf

UNDERSTANDING THE RISK…

- Digital MFPs have been in circulation for more than 10 years.
- A digital MFP (copier/Printer) contains an embedded computer.
- Similar to any laptop computer, the controller has:
  - A processor
  - Memory
  - A network interface
  - A large capacity Hard disk drive
- Typically, The hard disk retains thousands of pages of image data from any copy, print, scan or fax.
- Does any of this surprise you?

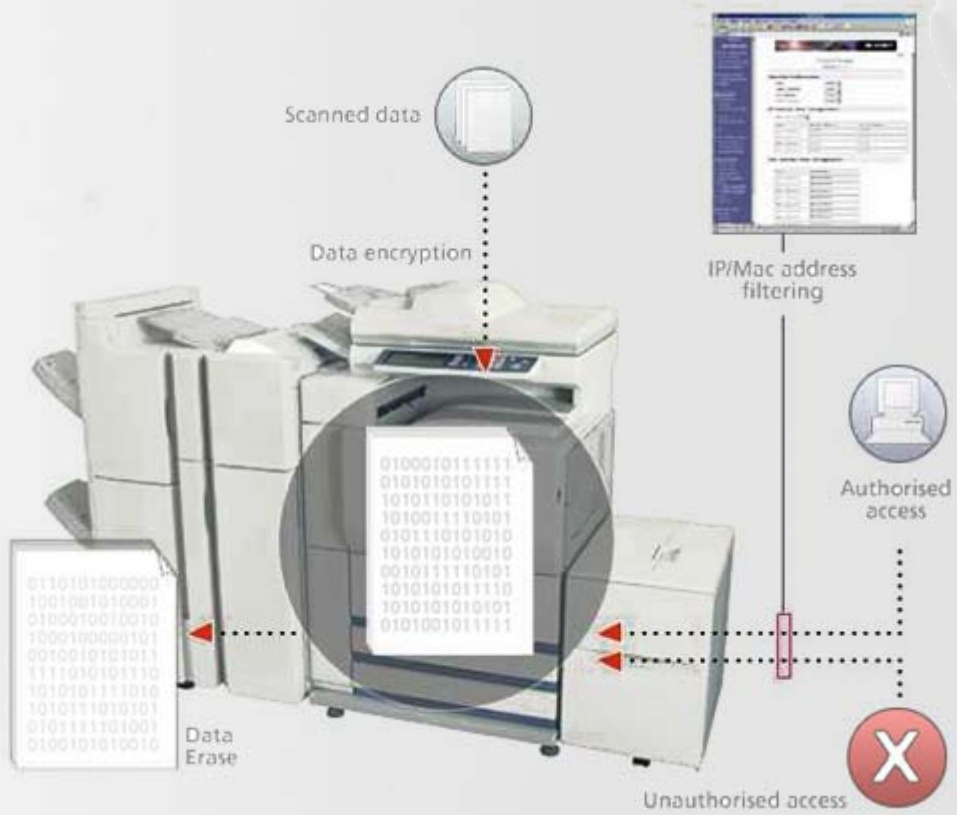
ACCEPTING THAT THE RISK APPLIES TO YOU!

Fact!	• Digital printers, copiers and multifunction devices have hard disks that still retain hundreds of pages of confidential data long after the document was created.
Fact!	• 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.
Fact!	• Documents that are left lying around in the output tray of your printer are open to being read by unauthorised personnel.
Fact!	• Copiers and MFPs provide a quick, untraceable means of copying and electronically distributing sensitive documents.
Fact!	• Documents sent in unencrypted emails by MFPs can be vulnerable to interception and/or incorrect delivery.
Fact!	• Information sent across a network to a printer of MFP is vulnerable to interception.

ELIMINATING THE RISK

Internal data encryption / hard disk erase

- **Copy Data**
- **Print Data**
- **Scan Data**
- **Fax Data**



Prevents data leak

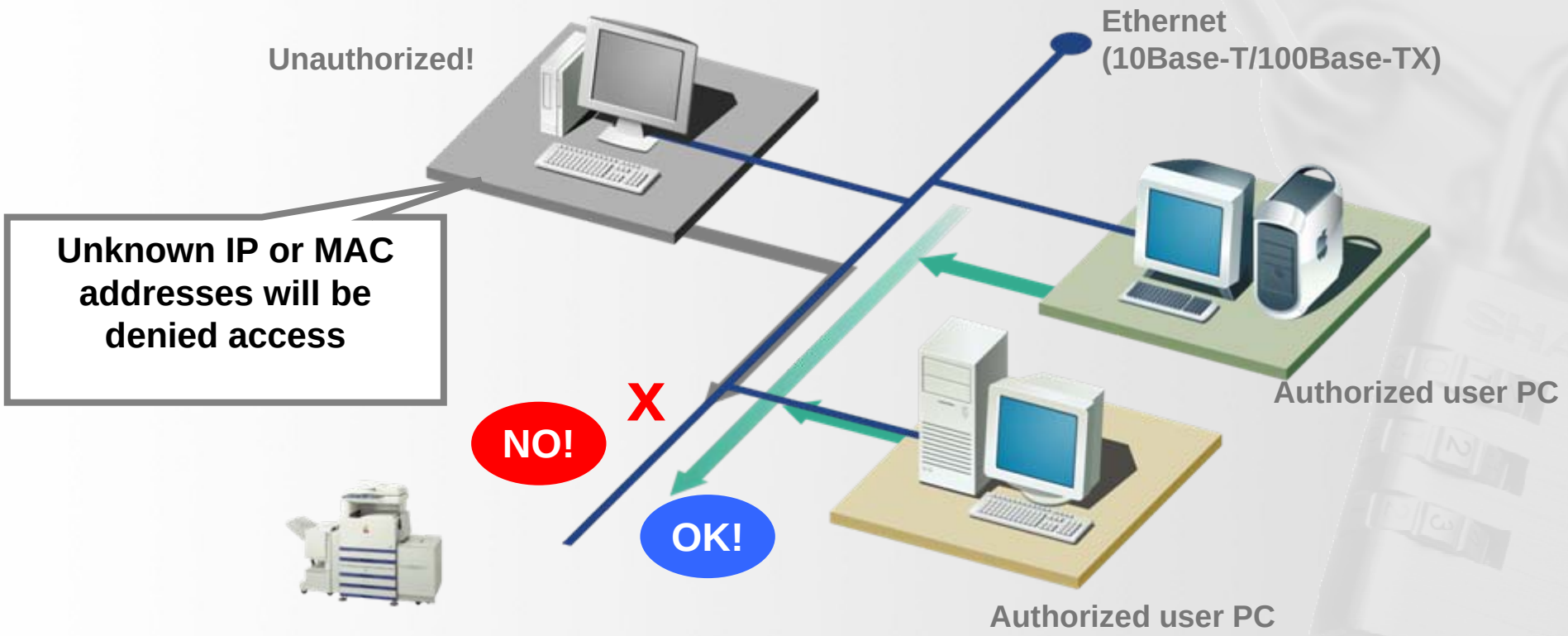
ELIMINATING THE RISK

Internal data encryption / hard disk erase

Video\English\3-2-2.swf

ELIMINATING THE RISK

IP/MAC Address Filtering



ELIMINATING THE RISK

IP/MAC Address Filtering

Video\English\3-3-2.swf

ELIMINATING THE RISK

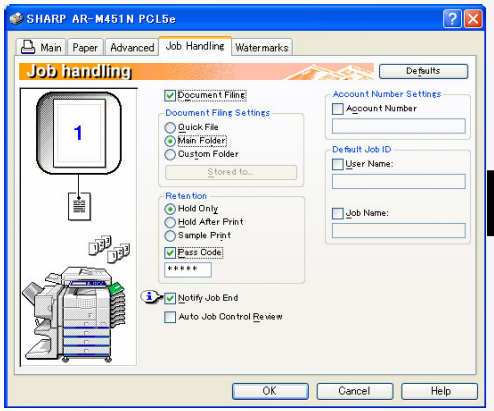
Confidential Print

Set PIN on your PC.
Data is sent from PC...

Enter PIN on
operation panel.

Confidential printouts
cannot be read by others.

*****



Confidential data in memory

ELIMINATING THE RISK

Confidential Print

Video\English\3-4.swf

ELIMINATING THE RISK

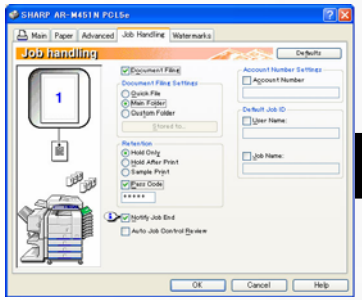
Network User Authentication

Before performing network scanning operations, a user must log into the machine using one of four types of authentication methods.

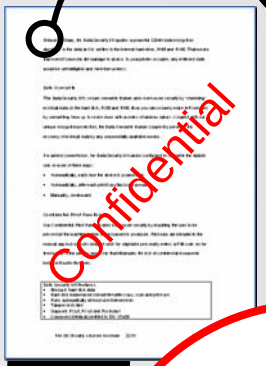
This prevents unauthorised access.

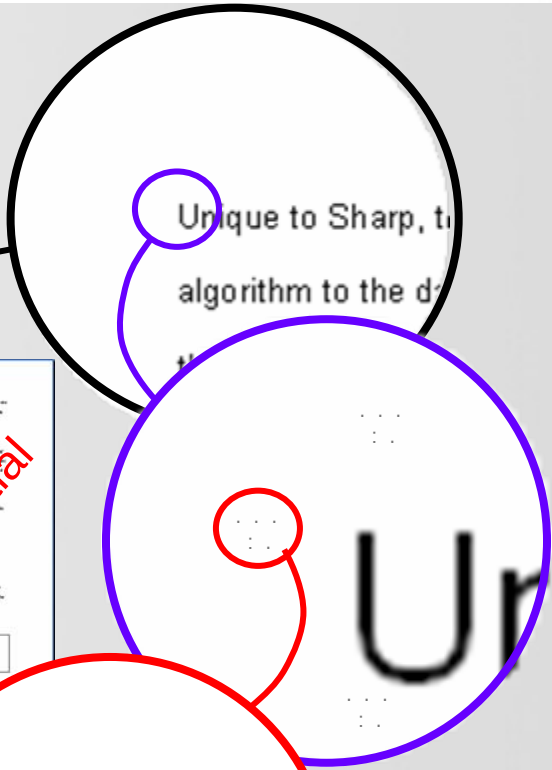
ELIMINATING THE RISK

Copy prevention



Printed document contains almost invisible markings





Copier can detect Markings and will stop the copy process!

X

No output!

ELIMINATING THE RISK

Network Data Encryption

- Protect print data and Web interface from eavesdropping
- Freely available Tools (for example: Ethereal) can capture network data
- Captured data can be played back (reproduced) or passwords can be extracted

- SSL (“Secure Socket Layer”)
- Encrypt the data streams across the networks
- Operation is mostly transparent to the user
- Uses “X.509 certificates” for key handling

THANK YOU