Ricoh Copier and Multi-Function Printer (MFP) Security

There have been several recent reports regarding photocopier and Multi-Function Printer (MFP) security. All copiers and MFPs today have hard drives which store images of the data received via copying, printing and scanning activities. Unfortunately, when copiers are re-sold or returned at the end of a lease, much of this data remains on the hard drive.

The University Information Security Office (UISO) has coordinated with Purchasing and met with our copier vendor, Ricoh, to determine what our options are for ensuring that a data breach does not occur due to this issue. University copiers and MFPs are leased on a co-terminus cycle and all are up for replacement in the summer of 2011. We currently have approximately 115 devices from Ricoh, our vendor, *76 of which currently have hard drives*. There could also be an unknown number of devices that could have been purchased by departments individually. We would have to do a survey of departments to determine whether there were any non-standard devices.

There are several options that are available to the University at varying costs. We have outlined a complete list of our options, along with a series of solutions the University can consider based on the amount of risk and cost that can be assumed.

SECURITY OPTIONS

Data Overwrite Security System (DOSS) Option ($212/per device)
DOSS overwrites the sector of the hard drive used for data processing after the completion of each (copy/print/scan) job. DOSS also offers the option of overwriting the entire hard drive up to nine times at the end of a lease or in the event a device is moved. The disadvantage of this offering is that documents cannot be stored on the device even if the department wishes to do so.

Hard Drive Encryption Option
If a drive needs to store data, the best option for securing that data is to encrypt the drive. However, this option may result in less usability of the drive and may not protect the drive from online attacks.

Network Security Features
Features such as user authentication, network communication encryption and the ability to close unused network ports.

Hard Drive Surrender Service (HDSS) Option ($250/per device)
Prior to the device being removed from the site, the hard drive is removed and provided to the customer for secure disposal.

Unsecured file deletion prior to disposal/transfer (cost to be negotiated)
There is an additional option to delete files prior to a device's disposal or internal transfer. However, if the hard drive were to be acquired by someone looking for files with sensitive information, it would be a trivial matter to recover those files. This option would be recommended for internal transfers of devices between departments.

SOLUTION SCENARIOS

There are four solutions that could meet our needs:

1. Purchase the DOSS and HDSS options for all devices. *Total cost: $35,112*.
2. Purchase just the DOSS option for all devices. *Total cost: $16,112*.
3. Purchase just the HDSS option for all devices. *Total cost: $19,000*.
4. Purchase just the DOSS or HDSS option for High Risk departments (approx. 25 devices). *Total Cost: $5,300-$6,250.*
    - *High Risk departments are those known to process data such as social security numbers, sensitive student/personnel data, and medical information. Individual academic departments are generally excluded from this category, although they do all process FERPA data.*

RECOMMENDATION

It is recommended that the DOSS option be purchased for all devices at a cost of $35,112. This cost may be negotiable with the vendor for such a large number of devices. For future copier/MFP purchases, it would be recommended that pricing be negotiated with the vendor for the configuration of Network Security Features including disabling any services that are not required in our environment.

It is additionally recommended that a survey of departments be conducted to determine whether or not there are non-standard devices that need to be addressed.