

Your documents are only as secure as your weakest link



In this high-tech, post 9/11 electronic age, companies are spending millions to lock down their networks with firewalls and antivirus programs. But safeguarding the most critical business asset--the information and knowledge found in your documents--is often overlooked. What's the point of bolting the door to your network if you've left the window wide open?

Whether it's a patent application, sensitive contract or a document with federally-protected employee information, it should be safeguarded from malicious network eavesdroppers or even accidental viewing from an unauthorized employee.

Lexmark Confidential.

Lexmark multifunction products have security features to help protect your documents.

Confidential Print.

It's a common concern in a networked office: What if someone views or picks up your confidential print job before you get to the printer? Confidential Print allows print jobs to be sent and held in the print queue until the creator enters a four-digit PIN number at the device.

PrintCryption.

Jobs are encrypted between the print server and the printer to limit exposure to network eavesdroppers. The data can't be simply interpreted by anyone who may be eavesdropping on the network.

Secure User Log On.

To prevent malicious use of the multifunction device by an unauthorized or anonymous employee, users may be required to log-in prior to performing a task. This technology reduces the risk that a user could send an anonymous email from the multifunction device across your network or the web. Instead, once a user logs in, his identity is known by the recipient. This feature also creates an audit trail, allowing companies to track when and by whom documents are copied, faxed, scanned or printed.

The potential for a security break is higher than you may think.

In spite of advances in digital technologies, the vast majority – 90 percent – of all office documents are still stored on paper.

An average document will be converted from paper to digital or digital to paper 19 times during the course of its life, creating multiple opportunities for a security breach to occur.¹

¹Source: AIIIM

SECURITY

www.lexmark.com