

MFP Security Loopholes

If your business is leasing MFPs from a third party, you should be particularly aware of the risk that the next customer may be able to see your confidential documents. Thinking of upgrading your own MFPs? Before you dispose of them, ensure that the data stored on them is deleted securely.

The use of multi functional printers (MFPs) has brought convenience and speed to business as well as potential security risks. MFPs are networked and have hard drives just like PCs which store data, e.g. IDs and previously copied/scanned documents. As a result, this data can be leaked in a number of ways, e.g. through paper copies and via the scan-to-email facility.

Every device added to a network must be evaluated in terms of security. For example, is the device going to have access to confidential data? Is it going to introduce any vulnerabilities to the network? How is access going to be controlled?

Just like network security, MFP security should be all about multiple protection layers. Start by evaluating the level of security appropriate for your business - is a standard level of security sufficient or are you subject to regulations which mean that your business needs to comply with heightened security requirements? The guidelines below can help business to deploy, manage and use MFPs in a secure manner whatever your security requirements.

User Access

Access to the MFP can be controlled through the use of authentication methods in a similar fashion as to when logging onto a networked PC. This feature prevents anonymous use of the scan to email facility and provides an auditing trail.

Output Security

How many times have you printed something fully intending to go and collect it immediately only to be distracted by a phone call in the meantime and the print out ended up sitting in the output tray? Output can be secured through the use of PINs at both ends - when sending the printing job from a PC and in order to print it at the MFP display panel. This way, the print job is generated only when the sender is standing next to the printer.

Network Security

MFP manufacturers try to make life for owners as easy as possible and many even offer to automatically send replacement toner cartridges when they start running low. This is all very good - just remember that you are giving access to your data to another party and introducing a potential way in for hackers. Disabling this feature, activating IP filtering so that only authorised devices can gain access and disabling incoming Internet access can all reduce outside threats.

Auditing Trail

If your business is subject to regulatory requirements you may need to keep an audit trail of every page that has been printed, scanned or copied. More sophisticated MFPs can generate reports by users, department or even billing code.

Data Security

MFPs have hard drives just like PCs - they can store user IDs, document images and configuration information, etc. It is not sufficient to simply format or delete stored data as this can be recovered fairly easily using commercially available tools. Document encryption, degaussing and shredding are methods that can be deployed to ensure that your data stays confidential at all times even past the useful life of the MFP.