



Information Security

Keeping MFDs watertight

The uninhibited flow of information within today's business environment has become a prerequisite of an organisation's success and smooth operation. But within every organisation, some of that information will be sensitive, and ensuring its safekeeping involves a comprehensive security policy. Like water coursing through a pressurised system, information has an unnerving habit of 'leaking' out through unchecked weak spots which have been identified and exploited by unscrupulous individuals.

And as with a pipeline supply of water, these leaks can go undetected for some time. The consequent damage is at best inconvenient, at worst catastrophic.

So far, so obvious, you may think. But NewField IT has uncovered a significant weak spot in many companies' security policy. Although there is an ever greater emphasis in IT departments on firewalls and PC protection, the multi-functional device - ie the combination copier, printer, fax and scanner - is, more often than not, completely overlooked. NewField IT's review of 41,000 hard copy devices, servicing 105,000 users, found sketchy or nonexistent policies in place to deal with the potential for information 'leakage' by these machines. Yet the risk is not only real, it is growing, with more and more organisations now rationalising the number of single hard copy devices, and investing instead in ever more sophisticated MFDs.

In order to help manage the risks, this White Paper sets out to explain why MFDs might be weak points in the system, and examines the options for a security policy which keeps the technology watertight.

UNDERSTANDING THE RISK

The greatest security risk posed by MFDs stems from the fact that most modern devices (and some mid to high-end printers) incorporate a comparatively large hard disk, many upwards of 40GB. This not only temporarily stores potentially sensitive

information which has recently been scanned, copied or printed, it also houses operating systems which are capable of running multiple software applications.

For example many of the more sophisticated models now incorporate a web interface - useful for administrators to see the status of a device, but this application also provides a potential means by which the device can be controlled. In many ways, an MFD is therefore not dissimilar to a standard PC, and if PCs are security protected, why not MFDs?

Happily, the historical problem posed by the fact that MFDs contained fax cards which potentially provided a route via the machine into the network, has been addressed and eliminated by all major manufacturers.

HOW REAL IS THE RISK?

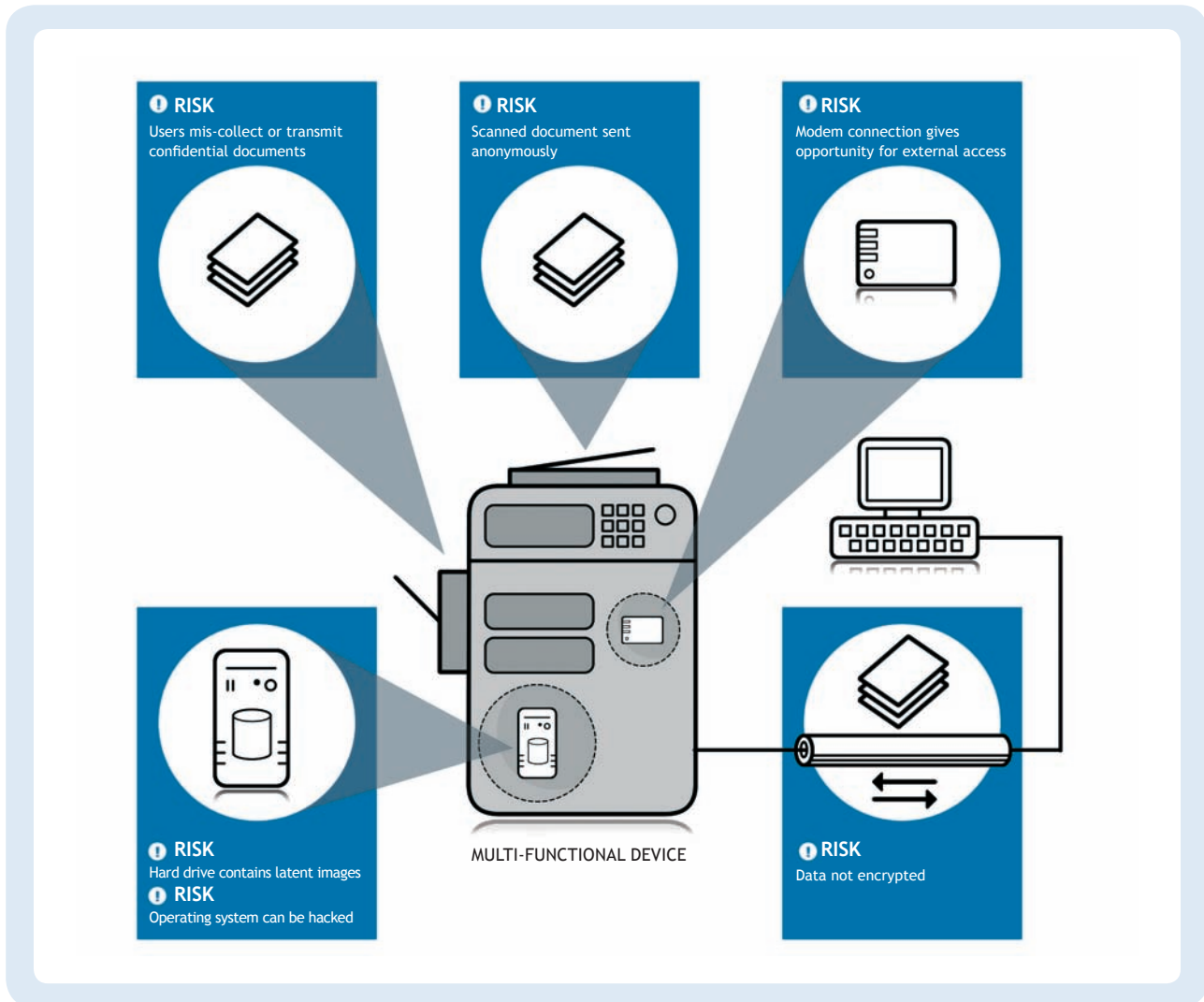
The reality of the risk has recently been evidenced by the fact that the two leading suppliers of MFDs released patches in 2006 for some of their devices following the exposure of security vulnerabilities. In both cases, the machines could be controlled following an internally generated attack.

Out in the workplace, there have been reports of MFDs being used to run web servers, whilst elsewhere, the unmanaged scan to email function is allowing users to send information anonymously both internally and externally. Recently, one global company discovered that users were sending information externally from an MFD only when a user rang the help desk to ask about additional features! For investment banks working on high profile cases and under ever tighter regulatory compliance, such anonymous leakage can have a hugely damaging economic impact.

Yet another potential risk is posed by the possibility that internal hackers could hack into an MFD in the HR department and gain sensitive information that has recently been scanned, copied or printed.

PREVENTING LEAKAGE

There are four key areas to security around the use of MFDs which if addressed will ensure the MFD is as safe as any PC within the network. The diagram below gives an anatomy of the weak points of an MFD:



1 The Document

Personnel picking up a confidential document from a shared MFD or printer probably remains the greatest risk for information leakage in most organisations. According to our research 89% of staff in a typical organisation say they produce some confidential information and 46% report experiencing the loss of a document on a shared device.

But there are three ways documents can be kept secure so that they are printed only when the user is ready to collect the job:

Print to an electronic mailbox. The MFD printer driver has a number mailboxes and each one can be assigned to a user with a password or a PIN. When the user arrives at the MFD console they can enter the password (or PIN) and select one or all documents stored for printing.

A slightly more cumbersome process is to attach a password to the document and then go to the MFD console to find the document and type in the password, thereby releasing the print job.

The most scalable and user friendly way is for the user to print in the normal way, but for the job to be held on the print server until the user identifies him or herself at any device and the job is sent to that device. This is sometimes known as 'pull printing'.

In addition to ensuring confidentiality, a secure release process for printing at MFD's also reduces waste (unprinted jobs can be automatically deleted after a certain time period) and reduces waiting time as if one machine is down or busy, the user can simply use another.

2 The Device

There are a number of potential vulnerabilities for the device itself which need to be addressed by a security policy:

Temporary images of print jobs which are stored on the hard disk can be overwritten and all residual data removed. The US Government has certification programme called the Common Criteria Evaluation and Validation Scheme to assess how well this is done. The standard is for a three pass overwrite with random data.

Also vulnerable is the operating system and application software running on the hard disk of the device. This is the area where some manufacturers have been exposed recently, yet this is a risk for all network devices and the issue is about treating MFDs in the same way as other workstations and applying the same security procedures - password protecting administration rights and keeping the firmware up to date.

Discarded devices can retain sensitive information on the hard disks, and the disposal procedure for MFDs must be the same as that of PCs, with the hard disk always being wiped as a precaution.

The bridge between the fax line and the device's network interface has historically been the weak spot of such devices. However, all major manufacturers have now addressed this issue but this should be checked prior to purchase.

3 The User

A key deterrent to information leakage is to create an audit trail which keeps tabs on exactly who has been using the MFD - and why. This is particularly important where information can be sent externally from the organisation via fax or scans to an email address. MFDs can be set up to identify a user in a two ways:

Users can type a name and a password into the MFD console, (standard windows login details can be used) before initiating any activity; this can be remotely configured by an administrator but it has the drawback of being time consuming for users and is likely to increase waiting time at the device

A staff card can be used to identify individuals so no extra passwords or manual data entry is required; this requires either embedded hardware for contact less cards or an external card reader for cards with magnetic stripes.

4 Distribution

In many ways, an MFD is a digital gateway into and out of the network for documents. So the way information is received and sent from it raises yet further important security issues.

For example, many MFDs come with a standard scan to email function and most companies don't realise that once the MFD is linked to the email server with its anonymous email address (usually MFD1@xyz.com) then emails can be sent externally without reference to any user. However, this can be easily addressed by limiting the users to selecting internal email address for the scan, and disabling the ability to manually type in an email address.

Strengthening yet another potential weak spot - the transmission itself - many manufacturers are now offering the option to encrypt information to be transmitted from the MFD and to use Secure Socket Layer (SSL) to ensure secure transmission.

CREATING AN MFD SECURITY POLICY

Of course, IT departments have happily installed and run printers with hard disks over the years, and managing the increased risks posed by MFDs should not be problematic. However, it is essential that organisations seek advice on how best to extend their existing security policy to ensure that by streamlining their provision of hard copy devices, they are not unwittingly weakening the overall security of their IT system.

The five golden rules are:

- Ensure users identify themselves
- Lock down the machines administration rights
- Keep the firmware up to date
- Have a standard for the device settings
- Dispose of them in the same way as PC's

Drawing on the above guidelines, it should be perfectly possible to create a policy which balances the desire for a watertight system against the need to maintain an uninterrupted flow of essential information.

NewField IT

■■■■ Print Management Architects

About the author: Robert Newry is a Director and Co-Founder of NewField IT, a specialist print management consultancy. NewField IT is leading provider of print assessments in the UK and has collected data on print usage at more than 30 different organisations, varying from public sector to large international companies.

For more information: visit NewField IT's website www.newfieldit.com or call 0208 948 9565.