

MULTI-FUNCTIONAL DEVICES

MARCH 2011

This note is based upon a research document compiled on behalf of CPNI by Deloitte. The findings presented here have been subjected to an extensive peer review process involving technical advisers from CPNI, our information exchange groups and wider industry.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Contents

INTRODUCTION.....	3
PURPOSE AND AIM OF THIS DOCUMENT	3
SCOPE.....	3
ASSUMPTIONS.....	3
EXECUTIVE SUMMARY	4
WHAT ARE MULTI-FUNCTIONAL DEVICES (MFDS)?	6
BASIC CATEGORIES	6
BASIC ANATOMY OF A MODERN MFD	7
KEY CHARACTERISTICS	7
BENEFITS OF MFDS	8
VENDORS.....	8
SPECIFICATION.....	8
PHYSICAL ACCESS.....	9
POTENTIAL SECURITY ISSUES	9
ACCESS TO PRINTED HARD COPY INFORMATION.....	10
RISK MITIGATION	10
LOGICAL ACCESS.....	13
CONSOLE ACCESS AND MISCONFIGURATION.....	13
WEAK AUTHENTICATION	13
'BACK DOORS'	13
REDUNDANT PROTOCOLS.....	13
RISK MITIGATION	14
COMMUNICATIONS SECURITY	16
NETWORK INTERCEPTION.....	16
EXFILTRATION	16
REMOTE MANAGEMENT PROTOCOL VULNERABILITIES.....	17
RISK MITIGATION	17
DESIGN AND ASSURANCE.....	19
SECURITY SPECIFICATION AND DESIGN ASSURANCE.....	19
OPERATIONS SECURITY AND ASSURANCE.....	19
RISK MITIGATION	20
ANNEX 1: VULNERABILITY MANAGEMENT	22
SOURCES OF INFORMATION.....	22
MAILING LISTS	22
ONLINE VULNERABILITY DATABASES	22
VULNERABILITY AGGREGATION AND MANAGEMENT SERVICES	23
MFV VENDOR WEBSITES.....	23
OTHER WEBSITES AND ONLINE RESOURCES	23
ANNEX 2: GLOSSARY	24

Introduction

Purpose and aim of this document

This briefing is to provide organisational management responsible for deploying multi-functional devices (MFDs) with an overview of the potential information security issues associated with deploying them. Its purpose is to raise awareness amongst the National Infrastructure community and provide some mitigation advice to the issues that are raised.

Scope

Modern MFDs have an underlying architecture that is comparable with stand-alone or networked computer systems. In many cases, the same information security issues, i.e. threats, vulnerabilities and protective security measures, applicable to these systems can also be applied to MFDs. This briefing is concerned with the Information Security issues specific to MFDs.

Assumptions

The following assumptions were made in the preparation of this document:

- The briefing is concerned with the threats and vulnerabilities associated with MFDs that are deployed in the workplace to perform copy, fax, scan and print operations.
- Effective governance and management of information security should encompass all aspects of physical, personnel and cyber security.

Executive summary

The term 'multi-functional device' (MFD) is typically used to describe the category of devices, whether used in the home or an office, which incorporate multiple document handling functions (e.g. copying, faxing, scanning, document storage or printing) into a single machine. MFDs range from peripheral devices found in the home to those that offer a wider range of high-speed reprographic functions over a network found in an office or print shop.

Modern MFDs have similar underlying functionality to standalone or network computer systems and consequently have similar information security threats, vulnerabilities and protective security measures. However, many are complex proprietary devices that because they may be deployed in an end-user environment give rise to different and sometimes complex security challenges. For example:

- **Poor security design:** MFDs frequently lack the security features found on computer systems. This is particularly evident in legacy products and those at the lower end of the consumer market. Many vendors do not include security information within their product specifications. However, the marketplace is changing and MFDs increasingly have advanced security features.
- **Lack of physical protection:** MFDs that are deployed in end-user environments often lack appropriate physical security controls. The devices are therefore vulnerable to unauthorised access and the theft of components, e.g. memory, hard discs, and system modification, e.g. configuration changes.
- **Proprietary designs:** MFDs are often designed to proprietary specifications and standards. As such, information on the available services and functions are not always documented or available to the customer. This aspect introduces the potential threat of unexpected and undocumented technical vulnerabilities.
- **External party risks:** In many organisations, the maintenance of MFDs is outsourced as this is often the most practical and economic way of maintaining them. This introduces threats such as unauthorised configuration changes, modification to hardware and software and/or unauthorised access to data that may have been stored on the device.

Potential threats may be mitigated by:

- **Limiting physical access:** The physical positioning of MFDs should be carefully considered to reduce the potential for unauthorised access or modification. The use of devices should be managed with the aid of appropriate organisational policies and procedures. Additional security systems such as CCTV could be introduced where the threat is considered to be sufficient to warrant such monitoring.
- **Limiting logical functionality and hardening access:** Where possible, unless implemented over secure communications channels, redundant and/or insecure system functions and protocols should be disabled to mitigate threats such as hacking, eavesdropping and man-in-the-middle attacks³. Strict controls should also be enforced at network interfaces such as disabling inbound fax from external sources as well as

³en.wikipedia.org/wiki/Man-in-the-middle_attack

anonymous e-mail sending. General best practice guidance on enforcing strong user passwords should be followed to provide resilience against password cracking attacks. Pre-programmed work flows could also be used to control complex user operations and reduce the potential for accidental data leakage.

- **Network segregation:** The threat associated with network attacks such as sniffing, malware and man-in-the-middle attacks can be mitigated to some degree by segregating MFDs from the main corporate network.
- **Encrypting data on disk:** Many MFD products are capable of encrypting data stored on internal hard drives and securely deleting data held in memory. Whilst this does not prevent the theft of storage components, assuming the technology has been correctly designed and implemented, these techniques can provide a level of assurance against the unauthorised disclosure of information.
- **Product evaluation:** Appropriate specification of requirements and formal evaluation of potential products during the procurement phase are critical steps in ensuring that MFDs are compliant with organisational security requirements. The inconsistency in MFD security standards and lack of vendor product information places greater importance on engaging with organisational security personnel.
- **Agreements with external parties:** Before decisions are made in any outsourcing situation it is vital the organisation carries out a thorough risk assessment. This is to ensure the organisation identifies the security requirement, as well as ensuring potential suppliers understand the risk they will be contracted to manage. Further CPNI advice on this topic can be found on the CPNI website⁴.
- **Effective governance:** Organisational policies, procedures, Service Level Agreements (SLAs) and monitoring processes should define and enforce security responsibilities and include:
 - Line management and user responsibilities;
 - Asset management procedures, which should include the marking of relevant internal components to detect the removal or installation of replacement parts;
 - Implementation of an information classification scheme and data handling procedures for hard copy material;
 - User training and awareness to educate users in operating the MFD and highlight the potential for any data leakage;
 - Regular review of log/audit information to detect unauthorised configuration changes and security breaches;
 - Disposal of redundant components or equipment;
 - Security incident management.

⁴ www.cpni.gov.uk/Docs/re-20060802-00524.pdf

What are multi-functional devices (MFDs)?

Basic categories

The term multi-functional device (MFDs) is typically used to describe the category of home and office products that incorporate multiple document handling functions (e.g. copying, faxing, scanning, document storage or printing) into a single device. MFDs range from peripheral print-scan devices typically found in the home to those that offer a wider range of reprographic functions over a network found in an office or reprographics facility. MFDs can be loosely grouped into the four categories shown below:

Type/Category	Characteristic
'All in One' device	<p>Desktop device, designed for home or home office use.</p> <p>'All-in-one' device generally focused on providing scan-to-fax, copy, scan and print functionality.</p> <p>May use removable media, e.g. SD Cards for photographs, etc.</p> <p>Locally connected by USB or possibly networked via WiFi.</p>
'Small Office/Home Office'	<p>Designed for small office or home office use.</p> <p>'All-in-one' devices generally focused on providing fax, copy, scan and print functionality.</p> <p>Document storage and retrieval.</p> <p>Networked with ability to connect locally by USB.</p>
'Office'	<p>Central printing function.</p> <p>Enhanced print, copy, scan, fax, document storage and retrieval.</p> <p>Network functionality and integration.</p> <p>Enhanced functionality such as scan-to-e-mail, e-mail-to-fax, etc.</p>
'Production printing'	<p>Designed for volume printing 'Office' MFD, optimised for high speed and quality output.</p> <p>Usually networked.</p> <p>Implemented in complex production workflows.</p>

Table 1: Basic categories of MFD

Basic anatomy of a modern MFD

The marketplace for MFD devices is changing rapidly as is the technology. MFD prices are falling as functionality increases. For the home or small office use, devices are normally proprietary and security is primarily physical. MFDs with more extensive functionality now increasingly use off the shelf operating systems with sophisticated security models comparable with that on computer systems.

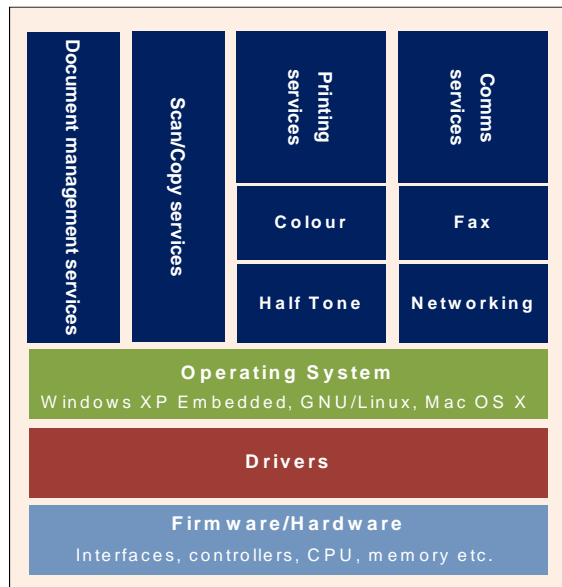


Figure 1: Basic computational layers of a modern MFD

At the hardware level, this includes components such as hardware controllers, interface cards, processors, memory (both persistent and dynamic) as well as communications components. The operating system includes device drivers, communications software and tailored user applications.

Key characteristics

Despite the similarities between MFDs and computer systems, they have a number of distinguishing characteristics:

- Applications residing on MFDs are principally geared towards the manipulation and distribution of data;
- Central reprographic and distribution functions;
- MFDs are frequently installed in end-user environments where security requirements may not be as rigorous as those found in computer rooms;

- Maintenance is often outsourced or the responsibility of another department within an organisation;
- MFDs are designed to proprietary security standards and specifications.

These characteristics have implications for information security and are explored in more detail throughout the rest of this briefing.

Benefits of MFDs

MFDs provide multiple functions and applications in a single device and thereby offer a number of benefits to the consumer, the most significant being the reduced cost of ownership compared with that of purchasing separate devices. They also enable organisations to be more operationally efficient, both in terms of document production and distribution, and the simplification of technical support.

Vendors

Several companies are developing MFDs and many models are re-badged. Most of these vendors offer a range of MFD solutions from basic copy/print devices to fully-fledged, high-speed reprographic solutions which provide copy, fax, scan, print and document management functionality across a network. Importantly, vendor understanding of the need for information security varies considerably between individual companies.

Specification

The specification of MFDs is developing rapidly as new technology emerges with those in the 'office' and 'production printing' market segments primarily differentiated by the quality of the reprographics output, compatibility and speed.

Physical access

As previously mentioned, MFDs are frequently installed in end-user environments and along with computer keyboards and system monitors, are viewed as part of the office furniture. As a result, users forget or ignore any security requirements. It should be emphasised that inadequate or uncontrolled physical access increases the potential threat significantly. This section discusses the security issues and provides some mitigation advice.

Potential security issues

MFDs, like most computer systems, are capable of storing significant amounts of data, either in memory or written to hard disc. MFDs are frequently seen as propriety equipment and maintained by external agencies through support contracts. In this operational environment, there are a number of potential issues to be considered:

- Engineers are employed by the maintenance organisation and without reference to the user organisation may change frequently;
- Depending on the organisational culture, whilst on the premises, engineers may be unescorted or escorted by personnel who are technically unaware of the engineer's actions;
- The engineers have total access to the MFD and may copy/delete data or make unauthorised modifications to its configuration without the knowledge or authority of the user organisation;
- Test equipment or media may be introduced which accidentally or otherwise introduces malware, thus compromising the confidentiality, availability and/or integrity of information stored or processed on the MFD;
- Uncontrolled updates to software and hardware may occur and as a result redundant or inoperative components that may contain sensitive corporate information may be removed from the premises without reference to the user organisation;
- When equipment or its memory components are replaced or become redundant, its disposal is outside the control of the user organisation and any data they contain may be disclosed to unauthorised personnel or agencies. Its loss may have a wide ranging impact for the organisation, for example in legal, financial, personal and commercial areas;
- Out of working hours, various personnel may also have unauthorised access to MFDs, e.g. cleaners, physical security and building services personnel.

Access to printed hard copy information

It is important to recognise that printing devices are a link within the overall security chain, since printers, copiers and MFDs produce the bulk of hardcopy business output, such as invoices, forms, tickets, statements, employee documents and customer data. Therefore, sensitive data is potentially vulnerable when in transit between a user's workstation or laptop and a printing device's output tray – particularly if printed remotely.

Some vendors have overcome the problem by developing products that require the intended recipient to authorise a print job on the MFD itself. One vendor requires a user to enter a personal identification number (PID) on the device to retrieve a document. Another has developed a solution whereby the user authorises printing using a smart card. The solutions allow users to print to a remote location where only a specified recipient can retrieve the document. A simpler solution may be to apply procedural controls for any hard copy output from the devices. However, any solution has to be practical and appropriate to the individual requirement.

Risk mitigation

Outsourcing Aspects

Before a decision is taken to outsource any maintenance or support process, any associated security risks should be assessed. This risk assessment is vital – to ensure that the organisation understands its security requirement, and to ensure that potential outsourcing suppliers understand the risk they will be contracted to manage.

Further CPNI advice on this topic can be found on the CPNI website at: www.cpni.gov.uk/Docs/re-20060802-00524.pdf.

Policy and procedural controls

In this context, technical solutions are frequently difficult to develop. Organisations may therefore have to rely upon operational policies and procedures. They should include as examples:

- All maintenance work should be supervised by appropriately trained personnel;
- Only previously approved personnel may have access to the building and the equipment;
- The disposal of defective or redundant components;
- Media updates and/or configuration changes will be subject to prior approval by the user organisation;
- Media control by the user organisation;
- Details of an information classification and document handling process.

Out-of-service maintenance and decommissioning

When MFDs are decommissioned, they should be subject to the same controls that are recommended for decommissioning of corporate computer systems. Any hard discs, memory components, media or hardware printing components which may have contained

sensitive corporate data should be removed and destroyed or overwritten to a satisfactory standard by the user organisation. In addition, any network configuration or user details which may be stored in the MFD should also be deleted.

Asset management

Organisations should implement asset management processes to ensure that MFDs and their internal components are properly accounted for. Components should be protectively marked and/or tamperproof evidence seals should be applied. Whilst this may not prevent theft, it can be helpful in detecting it and in recovering stolen parts. Any redundant media that could potentially contain sensitive data should be retained and disposed of by the user organisation.

Limiting functionality and hardening access

The risks associated with technical attacks on an MFD through physical access to the device can be mitigated to some degree by limiting functionality and hardening access. For example, as a general rule, access to menus involving configuration changes should be disabled or password protected.

Encrypting data on disk

In an MFD context, there are two main types of memory in use: temporary (e.g. Random Access Memory or RAM) and semi-permanent (e.g. solid-state drives or hard disk). Some MFDs are capable of 'securely' wiping data held in temporary memory and encrypting data held in semi-permanent memory. Whilst encryption cannot prevent theft, it can provide a level of assurance against disclosure when robust encryption algorithms and processes are used and decryption keys are secured against unauthorised access. MFDs which securely wipe data from temporary memory after use are also potentially less vulnerable to technical attack.

Diskless devices are also less vulnerable to data theft, however they may be limited in terms of functionality. This type of device is generally more suited to high security environments where the risk of data theft is unacceptably high and such devices offer the only alternative.

Local authentication of print jobs

MFDs which are capable of storing documents in memory until the users have authenticated themselves at the device provide an effective measure against sensitive data being left on a device's output-tray. These types of MFDs may be particularly appropriate in organisations where a single device is used to print and distribute different classifications of information.

Organisations can also implement procedural and operational controls to secure data in hard copy. For example, to support a classification policy, certain devices could be designated for printing sensitive data and loaded with protectively marked paper.

Overview of threats, vulnerabilities and mitigation advice

Threat	Vulnerability	Mitigation Advice
Disclosure of sensitive data.	MFD hard disk stolen, misplaced or subject to inappropriate disposal.	<ul style="list-style-type: none"> • Develop appropriate security policies and procedures. • Establish non-disclosure agreements and SLAs with outsourcing agencies and other external parties. • Securely wipe data which are no longer needed. • Suitably encrypt data held on semi-permanent memory. • Protectively mark internal components. • Apply tamper-evidence seals. • Deploy diskless MFDs in high risk areas (or use removable media that can be physically secured). • Suitably wipe or physically destroy memory components during decommissioning. • Supervise maintenance work with knowledgeable personnel.
Disclosure of sensitive data.	MFD security controls can be disabled enabling unauthorised logical access.	<ul style="list-style-type: none"> • Develop appropriate security policies & procedures. • Regularly review log files & system configurations. • Supervise maintenance work with knowledgeable personnel. • Password controls and configuration management.
Disclosure of sensitive data and disruption to services.	Installation of malicious code via removable media, e.g. USB devices	<ul style="list-style-type: none"> • Disable disk storage. • Virus-check all media before use. • Disable boot by external devices (e.g. USB). • Password-protect MFD boot configurations to prevent unauthorised changes. • Periodic wiping & reinstallation of the MFD hard disk. • Segregate MFDs and from corporate network.
Security responsibility undefined, appropriately owned or assigned. Ineffective security governance leading to inappropriate usage and disclosure of data.	Security tasks are uncoordinated, vulnerabilities are not identified (systems are unpatched and vulnerable to attack).	<ul style="list-style-type: none"> • Identify security requirements & tasks. • Define appropriate organisational policies and procedures. • Assign responsibilities to appropriate personnel (e.g. system administrator, users, line management etc.). • Include external party security requirements in SLAs.
Unauthorised access to hard copy information	Uncontrolled access to printed material	<ul style="list-style-type: none"> • Develop organisational policies and procedures to ensure controlled access to printed material • Enforce technical controls requiring user authentication at the MFD to initiate printing.

Table 2: Summary of mitigating advice for physical access

Logical access

Logical access security in the context of MFDs refers to the policies, procedures and system controls which enable local or remote access to an MFD. It is particularly concerned with user access to the device itself and any remote services. Such remote services have the advantage of allowing administrators to manage and configure a large number of devices across a network quickly and easily but may also introduce various threats and vulnerabilities.

This chapter discusses the logical access security issues associated with MFD deployment and provides potential mitigation advice.

Console access and misconfiguration

MFDs have varying types of user interface which tend to be vendor- or device-specific. Whilst most are graphical user interfaces designed to be intuitive and user-oriented, the range of various solutions makes it difficult for users to develop familiarity with programming operations, resulting in misconfiguration and leakage of data. For example, a misconfiguration of a fax transmission or scan-to-e-mail operation can result in confidential information being sent to an unauthorised external recipient, or being stored, unintentionally on a remote shared filestore.

Weak authentication

Despite the benefits of remote services, many 'high-end' MFDs support basic protocols and services which do not encrypt user credentials and only offer limited protection against eavesdropping attacks. The issues concerning insecure protocols are discussed in more detail in the section '*Communications security*'.

'Back doors'

Modern MFDs are complex computing devices and as such there is potential for hardware and software vulnerabilities similar to those found on computer systems. Potentially, these vulnerabilities can be exploited should there be a desire to do so. For example, some MFDs have fax and data modems on the same internal electronic board. Theoretically, it is possible that the fax interface could be used as a 'back door' into the network and information accessed or re-routed to another device.

Redundant protocols

In the default state, many MFDs have numerous services and protocols enabled which allow organisations to quickly deploy a range of devices. However, leaving redundant services and protocols enabled increases the potential for electronic attack. For example, Telnet, SNMP, FTP and HTTP may be open on MFDs, allowing hackers to use printing services to penetrate the network, establish themselves as an administrator, locate stored documents and replay print jobs. Insecure protocols such as Telnet are also vulnerable to

man-in-the middle and eavesdropping attacks. The attacker, having once gained access to MFD services, could also perform other forms of attack on the network infrastructure - for example, by using the compromised MFD to scan other hosts on the network, or using an embedded web server to host a malicious website that phishes for user credentials.

Risk mitigation

To mitigate against the risks, MFDs and associated systems should be hardened from a security perspective to limit impact from potential threats and vulnerabilities. Security should be enforced through technical controls, policies, procedures and compliance checking. The following sections provide some advice on possible mitigations.

Limiting functionality and hardening access

There is very little current evidence in the public domain to suggest that fax and e-mail functionality on MFDs is being specifically targeted by attackers. However, by gaining access to this functionality an attacker could exfiltrate sensitive information by disguising it as e-mail or fax communications. User authentication should be enforced where possible and redundant protocols and services disabled. Best practice guidance in respect of passwords and MFDs should also be used.

In addition, pre-programmed workflows can be used to assist user operations, and controls can be applied at network interfaces (e.g. by disabling network relay features, incoming fax from external sources, anonymous e-mail sending and assigning the MFD a static e-mail address) to mitigate against the threat of accidental or malicious leakage. As an example, some MFDs can be configured to enforce restrictions on where data can be distributed, i.e. to internal mailboxes only.

Auditing and logging

Auditing information is critical in assisting administrators to investigate information security breaches. Logging and auditing capabilities should be enabled on MFDs and enforced through policies and procedures which require, as a minimum, periodic review of log information and timely investigation of any security breaches.

Network segregation

Some of the security issues associated with MFDs can be overcome to some degree by segregating devices from the main corporate network. In addition, if MFDs route their traffic through a common network gateway then all inbound and outbound data can be scanned at that point.

Overview of vulnerabilities, risks and mitigation advice

Threat	Vulnerability	Mitigation Advice
Exfiltration of sensitive data.	Accidental leakage of information arising from misconfiguration of an MFD.	<ul style="list-style-type: none"> • Develop appropriate policies and procedures. • User training and awareness. • Apply appropriate controls to prevent unauthorised changes to MFD configuration, e.g. menu passwords. • Enforce strict controls at the network interface (e.g. disable mail relay features and anonymous e-mail sending, assign the device a non-routable IP address).
Unauthorised access to MFD services and possible loss or compromise of sensitive data.	Redundant protocols and services available on the MFD.	<ul style="list-style-type: none"> • Develop appropriate policies and procedures. • Disable unused services and protocols. • Apply appropriate controls to prevent unauthorised changes to MFD configuration, e.g. menu passwords.
Security tasks in respect of MFD are not co-ordinated leaving device open to unauthorised access and potential compromise of sensitive data.	Security responsibilities have not been defined, appropriately owned or assigned. Security governance is ineffective.	<ul style="list-style-type: none"> • Identify security requirements and tasks. • Develop appropriate policies and procedures. Assign responsibilities to the appropriate personnel (e.g. security administrator, users, external personnel etc).
MFD is not maintained properly leaving device open to unauthorised access and potential compromise of sensitive data.	MFD vulnerabilities are not identified and are not patched.	<ul style="list-style-type: none"> • Develop appropriate policies and procedures. • Define within external party contracts and SLAs any security requirements in respect of MFD maintenance. • Ensure contractual obligations are enforced.

Table 3: Summary of logical access vulnerabilities, risks and mitigating advice

Communications security

E-mail, fax and scan-to-folder are common features on most modern MFDs, enabling users to communicate data across local and wide area networks. The security of the data is dependent upon the information security measures used to protect it. Some MFDs implement communications protocols which offer very limited security features and are vulnerable from sniffing (i.e. eavesdropping) and man-in-the-middle attacks. Additional consideration also needs to be given to the security of any printed output.

This chapter discusses the information security issues around MFD communications and provides guidance on how potential threats and vulnerabilities can be reduced.

Network interception

Printing protocols

There are a number of common printing protocols in use including Line Printer Daemon Protocol (LPD); the Internet Printing Protocol (IPP) (sometimes referred to as the Berkeley Printing System); and JetDirect (also referred to as AppSocket, Raw or PDL-datastream). There are also network printers which use the IPX, Appletalk and SMB protocols to send print information. These protocols offer very limited security, thus exposing print jobs to interception, i.e. sniffing or eavesdropping attacks.

File transfer

File transfer across a local network is a common feature found on MFDs offering scan-to-folder functionality. Whilst file transfers can usually establish secure communications between most computer servers, many of the 'high-end' MFDs deployed in open networks support protocols that offer limited security features such as the File Transfer Protocol (FTP). These protocols are also vulnerable to interception, i.e. sniffing or eavesdropping attacks.

E-mail

Another common feature found on most MFDs is e-mail transfer. This enables users to forward scanned documents to any e-mail address. A number of MFDs are capable of integrating with an external e-mail infrastructure (e.g. Microsoft Exchange Server) to send and suitably encrypt material. However, these products also support insecure e-mail communications such as Simple Mail Transfer Protocol (SMTP) and again are vulnerable to interception, i.e. sniffing or eavesdropping attacks.

Exfiltration

In addition to the risk of eavesdropping, e-mail or fax servers could also enable an attacker to exfiltrate data from a local network by disguising it as e-mail (or fax) communications, thereby overcoming the procedural controls which would normally be followed. However, there is limited evidence in the public domain to suggest that these types of attacks are currently of concern.

Remote management protocol vulnerabilities

Most MFDs support the Simple Network Management Protocol (SNMP) which permits configuration viewing and editing from a remote system. Earlier versions do not implement encryption and are therefore vulnerable to packet sniffing attacks which can allow an attacker to obtain authentication information. In addition, all versions of SNMP are subject to brute force and dictionary attacks for guessing community and authentication strings, authentication keys, encryption strings, or encryption keys, because they do not implement a challenge-response handshake.

SNMP is also commonly used over UDP which is connectionless, and therefore vulnerable to IP spoofing attacks. Versions are also subject to bypassing device access lists that might have been implemented to restrict SNMP access.

Risk mitigation

Encrypted communications

As previously mentioned, MFDs which offer no support for secure communication protocols expose organisations to potential sniffing (i.e. eavesdropping) and man-in-the middle attacks. However, some modern MFD Products are now capable of supporting secure protocols such as Secure Socket Layer (SSL).

Wherever possible, redundant MFD services should be disabled. For example, Simple Mail Transfer Protocol (SMTP) listeners and senders allow the sending of blind or anonymous e-mail that could be exploited to launch spam attacks on internal or external networks. For each of the MFDs primary applications, secure protocols, such as the Secure File Transfer Protocol (SFTP) or File Transfer Protocol – Secure (FTPS, FTP over SSL) for file transfer offer better security.

Remote management

Organisations should consider whether they require remote management for MFDs. If they decide to use SNMP for remote management of MFDs then SNMP version 3 should be deployed (where it is available) with cryptographic security enabled.

SNMP is often used for remote monitoring and administration of other infrastructure components such as routers, switches, and firewalls. Policies that govern the use and configuration of SNMP for these devices should also be applied to MFDs.

Product evaluation

Evaluating whether specific MFDs implement secure communications protocols is a critical step in making sure that MFDs can be configured to customer security requirements. Organisations can mitigate against many of the risks associated with eavesdropping and man-in-the-middle attacks by deploying MFDs which support protocols which strongly encrypt communications, including the initial exchange of user log-in credentials.

Overview of risks and mitigation advice

Threat	Vulnerability	Mitigation Advice
Unauthorised disclosure of file transfer data.	Eavesdropping of file transfer data or file transfer user credentials.	<ul style="list-style-type: none"> • Develop appropriate policies & procedures. • Enable or deploy MFDs that implement secure network protocols such as FTPS or SFTP. • Disable insecure network protocols / applications such as FTP. • Encrypt communication channel at the network routing level.
Unauthorised disclosure of file data transferred by email.	Eavesdropping of email.	<ul style="list-style-type: none"> • Develop appropriate policies & procedures. • Enable or deploy MFDs which support secure mail (Microsoft Exchange or SMTP over SSL). • Disable SMTP and other insecure mail protocols if not being used. • Encrypt communication channel at the network routing level.
Disclosure of printed information.	Eavesdropping of print jobs.	<ul style="list-style-type: none"> • Develop appropriate policies & procedures. • Enable or deploy an MFD that supports IPP over SSL. • Encrypt communication channel at the network routing level.
Unauthorised access to MFD configuration; potential access to user data on disk.	Eavesdropping of remote management user credentials.	<ul style="list-style-type: none"> • Disable SNMP versions 1 and 2. • Enable or deploy an MFD that supports SNMP version 3 or above. • Encrypt communication channel at the network routing level.

Table 4: Summary of communications vulnerabilities, risks and mitigation advice

Design and assurance

MFDs are designed to meet vendor specifications. Common information security standards and features are not provided, e.g. support for secure protocols and system patching. Nevertheless, MFDs are used to process sensitive corporate information.

This chapter discusses the threats and vulnerabilities in deploying MFDs, and provides guidance on how they may be identified and mitigated through the application of a rigorous requirements definition, testing against requirements, and implementation of operational procedures.

Security specification and design assurance

The deployment of MFD devices in the workplace creates a number of information security questions. It is therefore vital when procuring equipment that the technical – and more specifically, the security requirement – should also be considered, including both personnel and physical security aspects. Examples of some of the technical questions include:

- Which protocols are enabled?
- Is data stored on media suitably encrypted?
- How do users authenticate themselves to the device?
- Are admin controls complete and easy to use?
- Which vulnerability management and patching processes are available from the vendor?

Some MFDs now incorporate fully featured operating systems and therefore have more sophisticated security models with a higher level of security functionality. Organisations may want independent assurances over whether MFDs meet their technical and security specifications. This could be achieved by purchasing products that meet the Common Criteria (www.commoncriteriaportal.org/) certification. Independent but structured product testing can also help.

Operations security and assurance

The lack of technical security features in MFDs will mean that policies and procedures are needed to compensate for perceived product vulnerabilities. For example, while many devices are capable of storing documents until a user has authenticated a print job, organisations can also reduce the risk of unauthorised access to printed material by implementing and enforcing procedural controls such as the classification of documents and data handling procedures. Similarly, organisations can implement procedures to ensure that components are physically destroyed or securely wiped either periodically or during decommissioning.

Risk mitigation

Design assurance and product evaluation

Modern MFDs which incorporate mature security models typically do not present the same vulnerabilities present in older products. Organisations deploying MFDs need to be aware of potential vulnerabilities and source products which can be configured to meet their security requirements. This means that business functions involved in procuring equipment need to engage with security personnel in the decision-making process.

The table below summarises the main security considerations based on a current view of MFDs available on the market.

Security design characteristic	Security design considerations
Data access	<p>What access controls have been implemented? (e.g. network integrated or proprietary user access model).</p> <p>What level of control and transparency does a security administrator have over MFD user access rights and privileges?</p>
Data storage	<p>Does the MFD encrypt data held in persistent (hard disk) and temporary memory?</p> <p>Does the MFD securely wipe data that are no longer needed?</p> <p>Does the standard of encryption used provide adequate protection?</p>
Data communications	<p>Can insecure communication protocols be disabled?</p> <p>Does the MFD support secure communication protocols? (e.g. SSL, IPSec, SFTP, etc.</p> <p>Can unauthorised access to the network to which the MFD is connected be prevented?</p>
Logging and auditing	<p>Is the MFD capable of tracking individual user activities?</p> <p>Can logs be accessed and modified by unauthorised users</p> <p>Can log data be extracted, reviewed and used to trigger security alerts?</p>
Change and patch management	<p>Is the system capable of patching? Does this require WAN remote connection?</p>

Table 5: Summary of security design characteristics and considerations

Some vendors certify their MFDs against the Common Criteria to verify that their implementation meets a certain specified set of security requirements. The associated security documentation describes what has been evaluated and possibly identify security issues that will need to be addressed. Independent testing can also be carried out though this is often difficult in practice because of the proprietary designs of MFDs.

Operational procedures and controls

Product test reports, Common Criteria certification and user documentation can provide organisations with the assurance that a device can be configured to meet security requirements. However, post deployment assurance activities and operational policies and procedures are needed to ensure the security of the device is maintained.

Overview of risks and mitigation advice

Threat	Mitigation Advice
MFD does not meet its design specification	<ul style="list-style-type: none"> • Consideration of security in the selection and procurement of MFD products. Security criteria should be identified to reach informed, risk-based decisions. • Deploy MFDs that have been certified against Common Criteria or tested by an independent body • Carry out independent testing of the MFD device.
MFD has been inappropriately deployed or configured and does not meet security requirements	<ul style="list-style-type: none"> • Carry out post-deployment assurance to make sure that the MFD security configuration meets security requirements (e.g. regular review of MFD security configuration settings). • Implement compensating controls such as CCTV, external network monitoring and decommissioning processes.

Table 6: Summary of implementation and operational security risks and mitigation advice

Annex 1: Vulnerability management

Sources of information

Information about vulnerabilities in MFD devices is available from various online sources including mailing lists, vulnerability databases and vendor websites. Depending on its requirements, an organisation could use a combination of some or all of these sources as part of a vulnerability management strategy.

Mailing lists

Mailing lists are often the first place where vulnerabilities are publicly reported and discussed. They are a good source of information despite occasionally containing incomplete or contradictory information, or information spread across a long discussion on the list. A detailed list of security-related mailing lists can be found at seclists.org, and further, less widely distributed information about the latest threats can be found at security-related web forums, blogs and IRC channels.

Online vulnerability databases

Vulnerability databases aggregate and categorise vulnerability information in a more organised and searchable way than a mailing list. The most widely accepted way of classifying vulnerabilities is according to the list of Common Vulnerabilities and Exposures (CVE) available at cve.mitre.org. This assigns standardised identifiers to vulnerabilities, which are used in vulnerability reporting sources, including mailing lists, vulnerability databases and vendor websites.

Other well-known vulnerability databases include:

- US Government National Vulnerability Database (NVD) nvd.nist.gov
This website holds the US Government's repository of standards-based vulnerability management data. The NVD provides fix information for identifiers on the CVE list discussed above.
- United States Computer Emergency Readiness Team Vulnerability Notes Database www.kb.cert.org/vuls
- The Open Source Vulnerability Database www.osvdb.org

Vulnerability aggregation and management services

Vulnerability aggregators are organisations which provide similar information to that found on vulnerability databases. They may also provide additional services such as detailed analysis, verification and evaluation of the vulnerabilities, distribution of information not in the public domain, and paid services to aid organisations in managing and tracking vulnerabilities within their environment.

MFD vendor websites

MFD vendors may include product vulnerability information and patches on their websites.

For most organisations, good practice information security policy should mandate searching vulnerability databases or aggregation services on a regular basis to identify vulnerabilities specific to the deployed technology in the organisation. An organisation willing to pay for these services may receive updates about new issues in their environment without having to invest effort in monitoring the lists direct. Alternatively, organisations may identify these issues during the course of other information security efforts, such as regular penetration testing or vulnerability scanning.

Other websites and online resources

Further information on MFD vulnerabilities accessible on the internet can be found on dedicated interest websites. These could include sites aimed at 'hacker' communities, facilitating the distribution of vulnerability information in order to enable damaging or criminal activities. These could also include sites intended to propagate risk mitigation advice. Although these sites may be valuable, the information they contain typically does not come with any form of assurance over its validity. The sites themselves may also be ephemeral, with no guarantee that they will be maintained or updated. Therefore placing reliance on them as a source of information is not recommended. They may have value as a means of highlighting information that is already available from more reliable sources, however.

Annex 2: Glossary

BIOS	Basic Input / Output System
CCTV	Closed-circuit television
CNI	Critical National Infrastructure
CPU	Central Processing Unit
ENISA	European Network and Information Security Agency
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
IPP	Internet Printing Protocol
IPX	Internetwork Packet Exchange
LAN	Local Area Network
LPD	Line Printer Daemon Protocol
MFD	Multi-Functional Device
NDA	Non Disclosure Agreement
NIST	National Institute of Standards and Technology
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SMB	Server Message Block (also known as Common Internet File System, CIFS)
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
Vendor	An organisation that manufactures MFDs
VOIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network