

# A Practical Guide to Print Security

Ideal for Businesses of All Sizes

The print environment is often one which is ignored within organisations' IT security strategy; however it plays a vital role in keeping data safe. Modern Multifunction Devices (MFDs), or Multifunctional Printers (MFPs) as they are sometimes called, are devices that can print, copy and scan as well as increasingly being equipped with cloud connections to enable users to scan and print from cloud applications.

As such they are complex document processing hubs that can transfer data to devices on the company network, and are often equipped with built-in web servers. With confidential data such as invoices, customer information and employee documents regularly moving between the desktop, mobile device and the printer, it is important you understand the role the MFDs plays in the security chain. Securing your print infrastructure is not complex, but does require thought. The steps you take will vary depending on the size and needs of your business.

We have seen that in the UK, a large number of fines imposed by the Information Commissioner's Office (ICO) involved data loss generated from MFDs such as printed records or faxes.

Canon Europe Limited have written this guide following discussions with the ICO so that, as the Data Protection Act (DPA) states, "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". This is known as the seventh data protection principle and is explained in more detail on the ICO's website, [www.ico.gov.uk](http://www.ico.gov.uk)

The guide is intended to give businesses of all size practical advice in the area of print security from a vendor-neutral perspective. It should be emphasized that following it alone does not, and will not, ensure compliance with current or future DPA requirements.

## What's in it for you?

Breaches of data protection legislation could lead to your business incurring a fine of up to £500,000 in serious cases; importantly the largest fines issues to date were a result of a paper-based breach.

Third-party research reinforces the print security risk – 70% of organisations have suffered a print security breach, yet only 42% has placed significant effort into print security and only 15% of respondents are concerned about data loss through MFDs and printers<sup>1</sup>.

To reverse this trend, organisations need to understand the potential risk the print environment presents and develop an appropriate strategy. Whether your business is a small office with a shared printer or a large office with a series of networked MFDs it is important that you lower the risk of exposure to potential threats, including malicious attacks and accidental leakage.

There are measures you can put in place to prevent security breaches from happening or limit the damage if they do occur.

## The first step: assess the risk to your business

Before you can think about security processes, it is important to carry out a thorough risk assessment. Every organisation has a different risk profile based on its size, IT infrastructure and profile of the workforce. You should take into account the type of data your company holds, how it is used, shared and printed; in short you need to look at a document's complete lifecycle and ensure it is protected throughout its journey from document creation to disposal.

Once you have established how much data your company has to secure and the types of risks faced, you can begin to think about the appropriate security measures to put in place.

---

<sup>1</sup> *Closing the print security gap*, Quocirca, Oct 2011

## General checklist

Although the strategies you put in place will vary dependent on the size of your business, there are a few simple steps everyone should consider:

- Read the MFD manufacturer's configuration guide and talk to your service provider and ensure that you customise your MFD – disable the default settings and only implement the features that you need. For example if you do not need to allow employees to print from mobile devices as this is against company policy, disable this feature and focus on the threats that your company realistically faces.
- Education should be at the centre of any security strategy. Employees need to understand the risks and the consequences for a company that is careless, so they can play an active part in security.
- Minimise the risk of paper-based leaks by using 'Secure Job Release', a function that means print jobs are locked in a queue on the device until the corresponding user PIN is entered. Paper-based leaks are a significant threat and this is one of the simplest steps you can take to protect your organisation.
- Consider what happens to the device at the end of its life – would you simply throw away a laptop once you'd finished with it, or would you clean the hard drive to remove all your data such as photos and music? The hard drive of a printer must be erased and securely disposed of at the end of its life.
- To ensure the MFD is a secure link in the information flow, organisations should disable default passwords and ensure employees have strong, unique passwords which are changed every 90 days for accessing their print jobs.
- Utilise hard disk encryption or erase options for MFDs where additional security is needed when handling sensitive or confidential information.

## Large and medium sized enterprises

### What is the problem?

For large and medium sized enterprises, huge amounts of data pass through the office's multifunctional devices (MFDs) every day. Businesses often have multiple sites and offices that use segmented network architecture and a separate VLAN, so have very specific security requirements.

One of the on-going risks for security professionals is not just the threat of malicious attacks, but the insider threat. Be it a disgruntled ex-employee or simply human error – the risk of someone who has access to confidential information can be difficult to protect against.

### What can I do?

- Use 'Secure Job Release' – this means documents can only be picked up from the printer if the user has access to it through their corporate ID. Documents are protected from any contractors that may not have full security clearance who can stumble across documents that are left lying around
- Link your print management software to your existing data loss prevention (DLP) solution. This allows you to apply the same security policies to data flowing through the MFD, to minimise the exposure to risk
- Make use of semi-visible watermark technology to help classify sensitive documents and highlight what is vulnerable

Print management software is one area of vulnerability that is increasingly important, especially if your company operates a 'Bring Your Own Device' policy. You need to protect your print software in the same way as any other software otherwise it could be the subject of attacks.

### What can I do?

- Separate the print server from the network to protect traffic from interception. When documents are in transit from the PC or mobile device – via the print management software – to the MFD, they are at risk. By separating the print server from the network server, the IT department can limit and control what traffic is going over that part of the network – reducing the risk of attack.
- Encrypt all traffic. Encryption means you can ensure that data can only be accessed by authorised users. When a document is in transit to the printer, it is travelling from one server to another. Encryption ensures

that, if compromised, the data can only be seen by authorised people and will reduce the impact of the breach.

- Enable auditing software to ensure that jobs get logged securely. In some sectors this is an industry standard so this is worth checking.
- Make sure you update all patches. Your print server should be configured with defined security standards, and a security patch update procedure that tackles the latest vulnerabilities as they happen.
- Control network monitoring, a 'network sniffer' can read data travelling between the PC or mobile device and an MFD, exposing the print job and routing addresses. If not already enforced, organisations should monitor and investigate any packet sniffing or port scanning behavior on the network.

## Small Businesses

### What is the problem?

Many small businesses now need a similar IT infrastructure as medium or large organisations and cloud computing, shared resources and outsourcing help those with limited IT expertise in-house.

These approaches have the potential to make the organisation more open to risk. For example, by giving external companies access to confidential data or, if your business uses a shared MFD it is possible an employee from another organisation can pick up sensitive documents left on the output tray.

### What can I do?

- The physical security of an MFD should always be an important consideration in protecting you from attack, especially if you use a shared office space. MFDs need to be placed in a position where CCTV cameras view it so that malicious activity can be both detected and deterred.
- By enabling 'Secure Print', print jobs are sent to the device but locked in the print queue until the correct person authenticates themselves, this ensures that only your own employees can access sensitive information and documents cannot accidentally fall into the wrong hands.
- If you choose to outsource, make sure you assess any company that is handling your data for security credentials and track record to ensure you are using a reputable organisation (see next section).

## **Outsourced MPS providers**

### **What is the problem?**

Today, many businesses use Managed Print Services (MPS), outsourcing the management and optimisation of their document output fleet to a third party. This can be hugely helpful as it allows businesses to refocus on their core priorities. But security should also be a consideration here; you need to make sure that any third party used has the same level of security as you.

### **What can I do?**

- Make sure that any third party MPS provider is audited for security. If any issues do arise you can then address them appropriately.
- Ask your MPS provider to present copies of any security assessments.
- Visit the HQ of your MPS provider, use your own judgment and only entrust your print services to a reputable company.
- Check all contracts, which should be in writing and your MPS provider should be contracted to act wholly under your instruction and comply with the relevant Data Protection Act.
- Ensure that once your company stops working with any third party the hard drives are still contractually yours and all information is returned to you or securely disposed of.

## **Mobile devices**

### **What is the problem?**

With remote working and 'Bring Your Own Device' on the increase, many organisations are deploying mobile print solutions. This presents its own security challenges, but there are steps you can take to reduce potential data breaches.

### **What can I do?**

- Ensure the same print security settings are employed consistently across all devices - from desktop PC, to tablet and smartphone - through all-encompassing print management software. This ensures all devices are subject to the same security settings.
- Deploy a mobile print solution which enables employees to print securely from any device without installing a print driver.

## Education

### What is the problem?

Although effective security strategies are employed, employee mistakes can result in data losses so it is important to educate everyone within your organisation.

### What can I do?

- Ensure all employees are appropriately briefed and know how to use features such as PIN enabled printing so that features are used well and do not disrupt your organisation.
- Educate employees about the importance of secure passwords to make sure that all passwords used with both professional and personal sites are long and complex enough to be effective and safe.
- Educate employees so they all know the consequences of a security breach to your businesses to make sure they are engaged in keeping your business secure.
- DLP solutions can also be used to help educate employees about the importance of print security. Simple features like implementing a 'Are you sure you want to print?' question on high security documents force people to think about the sensitive information that they're committing to paper. This can be used to help strengthen procedures and encourage secure thinking.

## Further Information

### **CPNI**

Guidance document from the Centre of Protection of National Infrastructure on MFD security.

### **ENISA**

ENISA is the European Network and Information Security Agency and works for the EU Institutions and Member States. ENISA is the 'pace-setter' for information security in Europe and its website acts as a hub for information, best practice and knowledge in the field of information security.

### **Quocirca – Closing the print security gap**

Many organisations now rely on printing to support business processes in industries across all sectors. Networked printers and MFDs are integral to business networks and so must be protected. The *Closing the print security gap* report provides an overview of the inherent risks when operating in an insecure print environment, as well as recommendations on best practice when adopting an integrated information and print security strategy.

### **Canon Guide**

Multifunctional devices are much more than printers, they are computer servers in their own right. As such organisations should address the security of the MFD as part of their overall security strategy to protect the confidentiality, integrity and availability of networked systems. Canon Europe has created a guide to provide configuration settings for two typical scenarios so that business users can securely add an MFD solution based on best practice.