Output Security

Protecting printed and electronic output

Contents

SHARP

Introduction

The need to protect documents that are physically or electronically output from MFPs and Printers is an often overlooked area of information security..

Sharp defines Output Security as security that is related to print output as well as electronic output from Multifunction Printers (MFPs) or Printers. This category includes all printed documents and electronic images of information in transit from a PC to a printing device (including printing through dedicated print servers), scan (including scan-to-folder, scan-to-email, scan-to-cloud, scan-to-HDD) and fax.

In this White Paper we will examine:

The Background

Describes why Output Management is an often overlooked area of information security. It also highlights the potential vulnerabilities that every IT administrator needs to be aware of, including:

- The growing number of organisations that are consolidating their MFP/Printer fleets
- The growing number of connected users, who all need to be identified and managed
- The growing number of documents that are being output and need controlling
- The lack of tools to track and report on all output activities.

The Problem

Looks at the Output Management challenges that IT managers, end users and management in business organisations can face. These include managing user access to printed documents, tracking user activity, reporting activity, accessing print from mobile devices as well as scanning documents to multiple destinations and faxing documents outside the organisation.

It also includes some data research that demonstrates the complexity of the topic and the scale of the problem.

The Recommendations

Outlines a set of Sharp products (software solutions) as well as best practices that can help you build a secure output environment and prevent unauthorised access to MFP and Printer fleets and the documents (including electronic images of documents), copies, faxes, scans and prints that they produce and store.

It examines how Sharp can solve problems by helping you to:

- Choose the right solution that fits your requirements and helps build the strong pillars of your Print Security Policy. An Output Management system can control access, apply printing rules, restrict functionality and ensure accurate tracking and reporting of all documents that are output.
- Choosing the right solution provider for your Output Management and related output activities.

The Conclusion

Provides a summary of the topic that focuses on:

- The main business vulnerabilities created by every document output
- A summary of recommendations based on the Sharp Security Solutions
- The next steps required to build a consistent Print Security Policy, including reliable tools, that can be applied to all aspects of your business.

Background

When businesses list potential information security risks they rarely, if ever, think of networked MFPs and Printers as a problem – let alone printed documents.

> **According to research firm Quocirca, 60% of organisations have experienced at least one data breach due to unsecure printing practices, and the threat is real to both smaller and large businesses**[1].

However, even if you deploy security solutions to protect your data from high-tech hackers or cybercriminals it's not always enough.

Some of the most common violations are as simple as a printed document being picked up by the wrong person. If sensitive documents are left at a MFP/Printer for too long, anyone can get hold of them and use the information to their benefit, which could cause serious issues.

> **56% of enterprise companies ignore Printers in their endpoint security strategy**[2].

If you think about it from a potential thief's point of view – the output tray is by far the easiest target if they want to steal confidential information. So an often under-estimated challenge for IT administrators is to make sure that printed documents aren't left lying around on top of an unsecured MFP/Printer where they could fall into the wrong hands.

However, the challenges that every modern organisation faces in ensuring output security are becoming greater every day for a number of reasons:

1. Growing device fleets

The number of organisations consolidating their MFP and Printer fleets is growing and businesses are looking for unification and standardisation. This brings a number of challenges due to a lack of tools to control the MFP and Printer:

- Functionality
- Output
- Security (as part of the network).

2. Number of connected (networked) users

In some organisations the number of employees can be significant, reaching hundreds of users printing from 10 to more than 100 devices. Add to this the growing number of security regulations, such as GDPR, and the challenges can be considerable when it comes to:

- User authentication
- Managing user accounts (including controlling the number of connected users)
- Integrating users with existing office systems
- The limitations on how organisations can manage user-identifiable data in their systems, such as user redaction for GDPR compliance.

3. Number of printed documents to control

The ever multiplying number of users and average number of printed pages per user means that a significant number of output documents need to be controlled:

- Copied documents
- Printed documents
- Scanned documents
- Faxed documents
- Documents printed through Smartphones and Tablets (Mobile Printing / Bring Your Own Device – BYOD).

4. Lack of control tools

There is generally a lack of tools that can accurately track and report on all output.

Problem

Output Security should be recognised as one of the key focus points in every modern business that uses MFPs and Printers.

Providing the right tools

Research analysts highlight the need to implement sufficient tools and measures to handle multiple print files, across multiple print devices to serve multiple users.

Securing output access

The challenge for every IT administrator is how to handle multiple accounts and users registered in the company's network. The number of users obviously impacts the administrative workload. It also complicates the user management process as well as all of the output related user activities, such as copying, printing, scanning and faxing. So the challenge here is how to handle Output Security effectively.

Some of the most popular techniques, such as PINs, Logins and Passwords, Cards and Fobs, are efficient ways to secure document output. However, they can be a real nightmare for the IT administrator if they are implemented and managed poorly. Especially as many IT administrators are also looking to connect devices and their output with existing systems, such as Microsoft accounts.

Number of documents and unattended printouts

The growing number of printouts is a real challenge. This includes both traditional paper documents that are either printed or copied on the devices as well as electronic documents submitted to MFP/Printers through the business network or sent through scan and fax functions.

New regulations, such as GDPR, have also opened up a variety of questions about how to protect unattended printouts and how secure the personal information contained in all the above output communication channels actually is.

Understanding the risks

In order to provide effective protection it is important to fully understand the risks posed by different activities:

Copying

Copying used to be the most popular way of sharing documents in the 1980s and 1990s, but it has now been overtaken by printing. Even so, copying is still a key area to control through Output Management systems, especially for sensitive business documents.

Printing

Printing is obviously a very common way to distribute business documents today, however, there are numerous risks when the printing is not controlled or not under centralised governance. *These include:*

- Unsecured and uncontrolled access to MFPs and Printers, as well as device functions and features, e.g. hard drives
- Open access to printed documentation where all office users / employees (and possibly even visitors) can access unattended documents
- An inability to track and report on user activities, i.e. who has printed what during a selected period
- An inability to track and prevent user data breaches, which could result in significant fines/charges due to strict security regulations, e.g. GDPR
- An inability to track mobile users and printing from mobile devices, like Smartphones and Tablets.

Scanning

Scanning can add complications to the security process as documents can be scanned not only to network folders and emails, but also to external, cloud-based systems. *There is also the risk of:*

- Scanning business-sensitive documents to external destinations, i.e. scanning to personal rather than business email addresses
- Scanning to multiple folders, rather than to selected personal business folders or network folders, without an IT administrator approved document destination and structure
- Scanning without indexing, which could cause serious problems when trying to find and audit scanned documents and audit scan-related activity (scan output and scan destinations).

Faxing

Similarly to scanning, faxing could be a potential weak point in the company's Output Security strategy. Whatever the transmission method – analogue faxing or sending faxes over an email – faxed documents are exposed to the same level of security breaches as scanned documents.

Mobile printing – Bring Your Own Device (BYOD)

Mobility is perceived by many research companies as one of the pillars of printing in the future. However, it brings challenges to the business in how to integrate mobile printing solutions into a modern organisation or how to track and manage the activities of mobile users accurately. In addition, an important question is how a mobile print strategy fits into the organisation's overall strategy. Unfortunately, many companies don't recognise that employee mobility is a growing trend or real business requirement. So the need for Output Security in this area is often overlooked.

Tracking and reporting

A real problem for businesses is not only how secure their document output channels are, but also how they track and report all of their output information.

It is important that the Audit report is also accurate and secure:

- Who has access?
- Is the data accurate?
- Can it be redacted?
- Who manages the system?

Recommendations

It is very important to understand that Output Security is just one of many office security areas, which can vary from organisation to organisation.

Some businesses may decide that if their Network Security measures are taken seriously and implemented carefully then these will be sufficient. However, as their business grows the number of documents generated also grows – along with the related security challenges.

It requires a broader approach to security in which not only the network is secured, but also all output information and documents that are generated and shared outside of the organisation.

In other words, securing a network and connected peripherals is essential. Output Security is a natural step to enhance your Network Security, not only in large organisations, but also in fast growing SMEs.

Using Output Management / Print Management applications, like one of Sharp's Optimised Printing solutions or Optimised Scanning solutions, will help you secure all office output, integrate your devices with existing systems, i.e. Windows, as well as deploy a consistent Print and Scan Security Policy quickly.

The most important factor in Output Security is control, because everything you can control you can measure and then secure. Our systems give you full control of every output document or piece of information: copy, print, scan and fax.

Because of its seamless integration with your existing Printer fleet, Output Management saves you a lot of valuable time. For example, importing all users through Lightweight Directory Access Protocol (LDAP) is quick and easy. Everyone can be added, identified and integrated with the system within seconds. Moreover, all user credentials are transferred using Transport Layer Security (TLS) to help avoid interception.

However, the real beauty of this Output Management system is the advanced features that make the life of every IT administrator and end user much easier:

1.User authentication

This is the first and the most important factor in how you access an Output Management system. The software gives you multiple ways to identify the user and grant them access to the connected devices. The fastest and most popular ways today are proximity cards and fobs. These store all personal identifiable information, and authentication is done using a card reader installed on the device. IT administrators also have a choice of using a number of alternative authentication methods, like PIN, User Login and Password as well as Biometric readers.

There's also an opportunity to use existing cards that you may currently be using in your business to access buildings, selected departments or protected rooms. There are a number of card and card reader standards using various communication methods and frequencies. So, we advise you to contact our Solutions Consultants to choose the right system for your business.

2. Secure queue

When a document is sent to print through a laptop or PC in the normal way the communication between the driver on the PC and Output Management starts. Only registered users can print to the system and only through licensed devices that have been configured with the necessary software. The user sends the job to the Output Management server and, when logging on to the device (using a Proximity Card, PIN or User Login and Password), the system identifies them as a registered user with the rights to print.

3. Pull print

The facility to have a secure queue and job holding on a server has another very important benefit as it gives you the pull printing feature (also known as follow-me printing) through any connected device. So the end user can print from any device – located in a different department, different floor or even different building (if it is on the same network) – or any place where the Output Management system is installed.

Pull printing also means less print-related downtime for your business. When one of the printing devices is out of service or undergoing maintenance, you can simply walk to the nearest available device and print your jobs.

4. Automatic job deletion

An additional challenge for IT administrators is the large number of pages that are temporarily stored awaiting output or indexing. But not when Output Management is in use. Thanks to an automatic job deletion function, IT administrators can setup a document retention policy. For example, if a document was printed at 8am and not released on the device within 24 hours, it will be automatically deleted from the server queue. This feature is fully configurable and depends on each organisation's requirements.

5. Elimination of duplicated printouts

Another benefit of implementing Output Management solutions is the elimination of duplicated printouts. Following their authentication and login to the chosen device, users can see the whole list of submitted files. They can easily see if any of the documents were sent multiple times and decide which documents should be printed and which should be removed. In addition, users can decide to print and delete from the queue or print and still retain the document in the queue.

6. Secure scanning, faxing and copying

Output Management allows you to control all of the functionality available on the device. The copy, scan and fax activities are controlled through the same user access to the device, and all of these activities can be monitored accordingly. *In addition:*

- To communicate securely, Sharp devices use TLS protocol for SMTP and S/MIME email encryption to ensure secure email communication
- The LAN network interface component of the MFP controller is completely isolated from the Fax PSTN telephone line. This prevents potential attackers from gaining access to the internal systems of the MFP or the local network.

84% of organisations place security as the most important priority between now and 2025, and security expertise will be the leading supplier selection criteria for 58% of organisations.[3]

7. Tracking and reporting

For many organisations, tracking and reporting are the most important considerations. With an Output Management system all activities are tracked. Regardless of whether you are printing, scanning, copying or faxing, all of your jobs will be recorded in the system. Detailed reports can be generated based on your personal account, department or specific client billing option.

8. User redaction for GDPR

Article 17 of the GDPR gives detailed instructions on how to handle personal information. This includes "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay." With Sharp's Output Management system this is not a problem. It allows you to redact all user data and comply with these strict regulations. Even when user data has been removed, IT administrators can still use some print insights and statistics to generate usage reports.

9. Mobile printing

This is a very simple concept – users can print as usual using their Bring Your Own Device (BYOD) Smartphone or Tablet. IT administrators can decide which application is the best for their organisation. The Sharp Optimised Mobile application, due to its comprehensive configuration, can be tracked through Output Management, so all mobile-printed documents are reported in the system and can be used for statistics and generating reports.

Building even stronger security

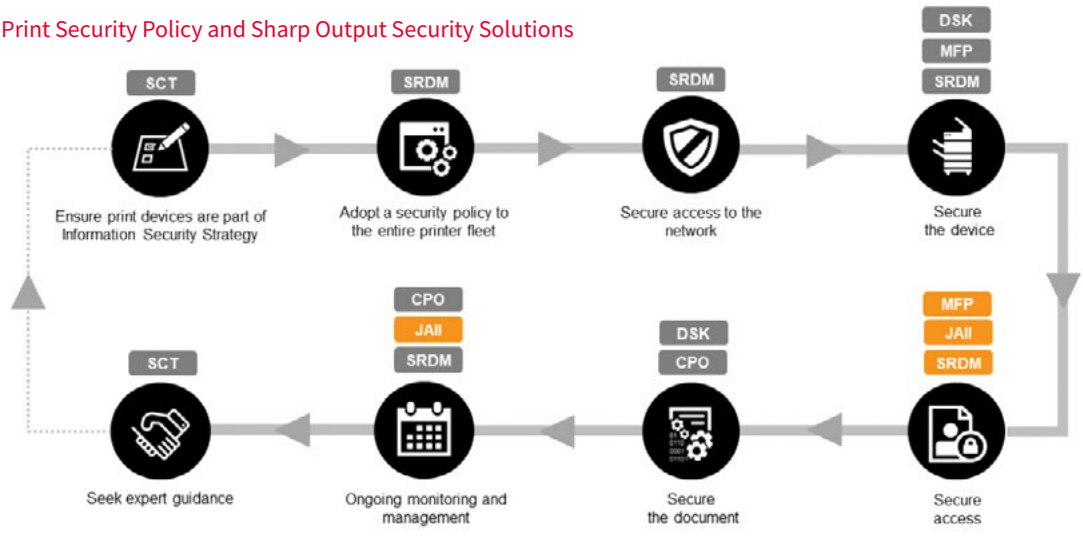
Output Security plays a very important role in defining, building and implementing your own Print Security Policy:

- **Output Management products from the Sharp Optimised Portfolio are extremely valuable when applying such a policy, mainly because it enhances the 'Securing access' and 'Ongoing monitoring and management' steps.**
- **Adding more products from our portfolio, like Sharp MFPs, Data Security Kit (DSK), Sharp Remote Device Manager (SRDM) and Cloud Portal Office (CPO) help you build a unique, robust and consistent security system that works perfectly for your IT team as well as for your business.**

So, to build the strongest possible levels of security, businesses should work with suppliers that can not only deliver tangible benefits in the area of Output Management, but are also trusted and experienced integrators.

Sharp has many years of experience in manufacturing the most secure MFP/Printers, developing Output Management applications and implementing complex solutions. So we are in a very strong position to advise and guide our customers on all aspects of security, including Print and Output Security policies.

Building Print Security Policy and Sharp Output Security Solutions



SCT – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Data Security Kit, **MFP** – Multifunction Printer, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Conclusion

The new business paradigm is that every time anyone prints, copies, scans or faxes a document it is vulnerable to being stolen or compromised.

Businesses need to be much more aware of the risks posed when physical or electronic copies of sensitive documents and files are left unprotected.

The key issues are:

- Output Security is essential for every modern business regardless of its size. The growing number of documents generated by companies brings significant challenges when controlling the IT environment. In particular, these include managing the increasing number of users, bigger files, the amount of information being shared, network overloads and the Printer fleet.
- An Output Management system gives you the maximum flexibility for configuration. IT administrators can not only restrict access to closed groups of office users, but also track all of their activity on the MFP, including copying, printing, scanning and faxing.
- Sharp understands how important security in the modern office is and offers a unique 360-degrees approach to this matter. From Network Security, which covers all business networks and all connected peripherals, to Output Security described in this White Paper, through to Document Security, which deals with all aspects of document-related security.

This comprehensive security approach ensures that your organisation also benefits from the highest level of compliance with the latest security regulations, including the General Data Protection Regulation (GDPR).

Sharp Security Framework

To avoid potential vulnerabilities in other areas of your business, we suggest that you learn about how to introduce further security measures related to:

- Network Security
- Output Security
- Document Security
- GDPR compliance

You can find more information on the above topics in our White Paper library or in the Information Security section on our website:

www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/information-security.htm

Alternatively contact your Sharp Solutions Consultant.

References

1. Print 2025: Print Security in the IoT Era. *Quocirca, 2018*
2. Annual Global IT Security Benchmark Tracking Study. *Ponemon Institute, March 2015*
3. Print 2025: The future of print in the digital workplace. *Quocirca, 2018*