Network Security

Protecting office network devices

Contents

SHARP

Introduction

In today's connected world, effective information security across the entire business network, has never been more vital.

Every day there are countless malicious attempts to steal, illegally modify, intercept, or disseminate confidential documents, or gain unauthorised access to private and business networks. This White Paper examines the key challenges that businesses face in protecting their IT infrastructure, in relation to networked office devices, such as Multifunction Printers (MFPs) and Printers.

In this White Paper we will examine:

The Background

Every business faces challenges from a network security perspective, but the vulnerabilities exposed by today's networked MFPs and Printers are often overlooked. Hackers and cybercrimals are using them as a route into organisations in order to steal confidential data stored on hard drives and other networked devices, and also cause malicious damage or disrupt business activities. The impact on productivity and profitability can be huge.

The Problem

The risk posed by unsecured MFPs and Printers is often misunderstood and ignored, or businesses simply lack the expertise and resources to start tackling the problem. A lack of awareness amongst users is also exacerbating the problem as bad practices needlessly expose documents and data to the risk of being compromised. Businesses understand the steps that they need to take to create a Print Security Policy, but it can be a complex and time-consuming process.

The Recommendations

We describe a set of hardware and software solutions as well as best practices that can help you build a secure print environment and prevent unauthorised access and attacks on business networked devices. This section includes specific answers to some of the key security challenges:

- Six steps to introduce and maintain print security standards, using a combination of Sharp technology and Sharp Optimised Software Solutions.
- 'Out of the box' features and settings available on every Sharp networked device in the current range, e.g. Password protection, Data Overwrite, Encryption, etc.
- Optional solutions that help you build a consistent Print Security Policy and manage Printer fleets easily and effectively, e.g. Sharp Remote Device Manager (SRDM)
- Optional MFP/Printer advanced functions and features e.g. Data Security Kit (DSK)
- Optional services available through the Sharp direct channel, e.g. Security Audit, Security-as-a-Service, End-of-lease data erase, etc.

The Conclusion

We provide a summary of the following:

- The findings on business vulnerabilities regarding every networked MFP and Printer
- Our recommendations based on the Sharp embedded features and additional Sharp Security Solutions
- The next steps required for building a Print Security Policy – either using an in-house approach or with the help and expertise of the Sharp Professional Services team.

Background

In recent years the need for effective IT security has gained much greater prominence – but one key area has been dangerously overlooked.

Most security-conscious organisations have ensured that their network and computing assets are protected with the latest technology: installing firewalls, enforcing password rules, requiring user authentication, as well as protecting encrypted and electronically signed data and more.

New technologies, such as cloud and mobile, brought additional challenges to IT administrators and security officers. However, today's intelligent MFPs and Printers have evolved to include many network communications and data storage capabilities. Basically, they have become powerful, smart-featured computers.

And, according to IDC, there are almost 53 million Printers and Multifunction devices in offices and homes throughout Western Europe and Eastern Europe[1], and most are connected to a network.

This means they are an access point with an IP address and are just as susceptible to malware and hacker attacks as PCs or any other network-connected endpoint. So, they require the same level of data, communication and information security features.

If MFPs are left unsecured, hackers could have access to uncontrolled ports and protocols, which would enable them to access other machines on the network or sensitive information. Communications and data stored on an MFP's hard disk drive or in memory could be intercepted or sent without permission anywhere in the world. The networked devices would also be open to Denial of Service (DoS) attacks, which are designed to make the network resources unavailable to end users, with a consequent impact on business productivity. They can also provide an open gateway for phishing attacks designed to obtain confidential information or the introduction of viruses onto the network.

And this isn't just hype – it is a very real threat. In a recent IDC survey more than 1 in 4 respondents indicated a significant IT security breach that required remediation, and more than 25% of these incidents involved print.[2]

Failing to protect MFPs and Printers may result in devastating damage to a business – as well as its reputation and customer trust.

The effects of a breach can include:

- **Loss of revenue**
- **Loss of productivity without access to data and the network**
- **Loss of competitiveness due to stolen information**
- **Fines due to regulatory non-compliance**
- **Lawsuits**
- **Unauthorised use of equipment and network resources.**

Problem

Hacker activities and cyber attacks have become the 'norm' and, regardless of your business type and size, the threat of malware activity impacting your operations is very real – and imminent.

> It may surprise you to know that, according to research firm Quocirca, 63% of businesses surveyed admit to experiencing one or more print-related data breaches[3].

So why haven't businesses done more to combat the threat?

Unfortunately, the potential risk is often overlooked due to a lack of understanding of the vulnerabilities that are created when devices such as MFPs and Printers are embedded into the business network. So many businesses either lack or have insufficient print security systems and tools, including trained people, best practices and security procedures relating to the use of networked devices in the business. Or they are using devices for business purposes that are really designed for home use and have limited security features.

In particular, small and medium size businesses may not have introduced any print security measures and/or never undertaken a print security audit. Bigger organisations may just have insufficient human resource or quality tools to measure, control and prevent cyber-attacks on network devices and connected technologies.

In addition, bad user practices are often a serious challenge for IT administrators as they can cause significant security problems for the business. These may include unsecured printing, leaving documents unattended on the MFP/Printer output trays, printing from unsecured USB drives, printing without endpoint to endpoint encryption or storing sensitive documents on the MFP/Printer hard drive.

For many organisations the disposal of data when a contract ends can also be a real problem. The printing process can leave an MFP/Printer hard drive with a copy of the data that has been printed on the device. So what happens to the data when contract ends?

Unfortunately, setting up a consistent network security system or introducing a Print Security Policy to detect and prevent unauthorised access to a fleet of networked MFPs and Printers can be a really complex and time-consuming task.

You will almost certainly need to go through the following key stages:

- Predict and evaluate any potential implications of not having a network security system
- Recognise the existence of potential vulnerabilities and how they could harm the network infrastructure
- Understand the complicated nature of the challenge, which will inevitably vary from business to business
- Find an internal or external resource to help you address the challenge
- Identify tools that can monitor entire fleets of MFPs/Printers, prevent unauthorised access to the networked assets and alert you to any suspect activities
- Set up and maintain a reliable network security system that encompasses all of the unique challenges faced by your business.

Recommendations

If all of this has made you concerned about your own network security then… OK! The risk to your business should not be underestimated. But don't be afraid.

Our aim is to present a simple way to introduce comprehensive print security measures to your business and indicate how Sharp can help understand and uplift your network security levels easily and without difficulty.

Turn On Instant Protection

Research by industry analysts IDC has shown that:

hardcopy managed print and document services technology suppliers are concentrating their efforts on print device security that prevents hackers from entering enterprise networks via print devices.[4]

However, many businesses overlook or do not set security settings properly, which can leave them vulnerable to attacks.

The following is a list of security features and settings that are available 'out of the box' on all Sharp MFPs and Printers, which can provide a 'quick fix'. All of them can be quickly switched on/off or adjusted by the IT administrator to change the default security levels and provide a much more effective level of protection for your particular business needs:

- Local administration settings including: Admin Password change, Device Webpage access, Remote Operation security
- Standard mode setup of security features: Port Controls, Protocol Settings, SNMP MIB setting, Access Filters, SSL, S/MIME, IPSEC, IEEE802.1X, Enable / Disable Mobile Print protocols , External Service Settings, Public Folder - Network addressed Server (shared disk), Tracking ID (Tracking information print), User Settings, Enable/Disable User security workarounds, Automatic deletion of stored files, Delete entire spool queue on error
- Enhanced security features (in Standard Security Mode): HDD Data Overwrite (Hard disk erase) after each Copy/Print/Scan/Fax, Storage Encryption, Password Protection
- In the same group there are several advanced, optional settings. These settings can give IT administrators access to advanced Sharp security features that are beneficial for organisations that require the highest security levels, such as military or government bodies, or any business that wants to uplift its security to the highest-level:
  - Data Security Kit (DSK) includes: Data Security Kit Installation, Data Security enhancements, Print Security enhancements, Firmware validation
  - Advanced Data Security Kit (Advanced DSK) includes: HCD-PP Certified Advanced Security mode (Includes Data Security Kit), Storage Encryption enhancement, Enhanced Password requirement, Firmware security checks

Six simple steps

Looking at security from a longer-term perspective, the following six steps offer a structured way to develop and introduce your own, consistent network security framework.

1. Secure access to the network

Any devices connected to the network are only as secure as the most vulnerable point on the network. So controlling the use of ports and protocols is a very important part of maintaining network security. Through sensible configuration, IT administrators can prevent unwanted activities and potential attacks on the infrastructure. The techniques for ensuring secure communication between each device and the network include:

- Use IP filtering to limit the access to specific IP addresses as well as MAC (Media Access Control) filtering. This helps to protect your network and your communication channels by only allowing access through specified IP addresses or ranges.
- Disabling unused ports (so only the required one's work) provides an extra security layer and gives you more control on your network, by preventing unauthorised access to all connected assets.
- Ensure that IPSec (the Internet Protocol Security for secure and encrypted data exchange), TLS (the Transport Layer Security for encrypted data transmission) and HTTPS (the Hypertext Transfer Protocol Secure for secure network communication) are configured for the highest protection level.

2. Secure the device *(to protect your data)*

There are two ways to ensure that the data stored on the hard disk drives (HDD) of MFPs and Printers remains secure:

- Data Encryption is the procedure or functionality that encrypts documents using a complex 256-bit algorithm
- Data Overwrite is the data erase option for a device's HDD. It ensures that all data already stored on the drive and any electronic images of printed documents are permanently erased by being over-written up to 10 times.

For added peace of mind, Sharp also offers an end-of-lease/service option that ensures that any digital data left on a device is erased and the physical HDD destroyed.

3. Secure user access *(through user identification and authorisation)*

One of the most important steps is to get all users under control by introducing user administration and authorisation. In this category the key activities consist of:

- User identification is the process through which administrators give only registered users access rights to MFPs and Printers. They must identify users using either local authentication, based on the local user list, or network authentication through the authentication server.
- User authorisation is used to grant access to the organisation's network assets and control their usage. Based on each user's credentials, they can limit the access to specific people, restrict access to device functions, or completely block access. The administrator can also configure access to the device through ID cards, which hold the user identification data.

4. Print confidential information securely

Confidential documents should only be printed using a secure procedure that prevents unauthorised access and copying. Typically, when a print job is submitted it will be held on the device's HDD and will only be released once the user enters a PIN code, which will have been previously configured. Once the document has been printed all data is automatically erased from the HDD.

5. Control network activity

When introduced correctly, network security tools can give IT administrators total control of all networked devices, directly from their desktops. So they can control an entire fleet of MFPs and Printers and also remotely discover, set up and manage most of the potential security threats. The ability to clone devices also streamlines the work of administrators and provides added peace of mind, as any changes to device settings can be easily populated across the entire fleet.

6.Choose the right partner

There are many companies offering professional services related to print security, however, the level of expertise can vary significantly. Sharp takes network security very seriously and is at the centre of every new product development. As a manufacturer, our equipment is evaluated using guidelines specified for comprehensive Common Criteria certification. As a result, our networked MFPs with an embedded data security option have been independently assessed by the globally renowned Japan's IT Security Evaluation and Certification system (JISEC). They have been certified as conforming to the latest Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0) standard of the Common Criteria, which means that we can support customers handling the most sensitive data in the world.

Get expert help

While all of this may seem rather daunting, it is important to remember that you are not alone – expert help is always available.

In particular, Sharp offers several solutions, tools and services to check and measure your network vulnerabilities, prepare the improvement plan and design possible scenarios available to you:

Print Security Workshop

We can utilise a number of tools and techniques that can help your organisation to understand the security threats, list the conclusions and build a tailored improvement plan.

The audit focuses on all networked peripherals and their security. We measure all standard and advanced features available for these devices as well as tools for effective threat discovery and prevention. We also check if the devices you use in your business are fit for purpose and can deliver maximum security protection for your business and users. In addition, the Print Security Audit outlines the 'next steps' to introduce a consistent Print Security Policy and cover all security aspects in your business, including:

- **Network Security** – as described in this document
- **Output Security** – covering all activities related to document output, such as printing, scanning, faxing and emailing
- **Document Security** – addressing the management of electronic and paper files used in your office
- **GDPR compliance** – ensuring compliance with the latest EU regulations on security and personal data protection.

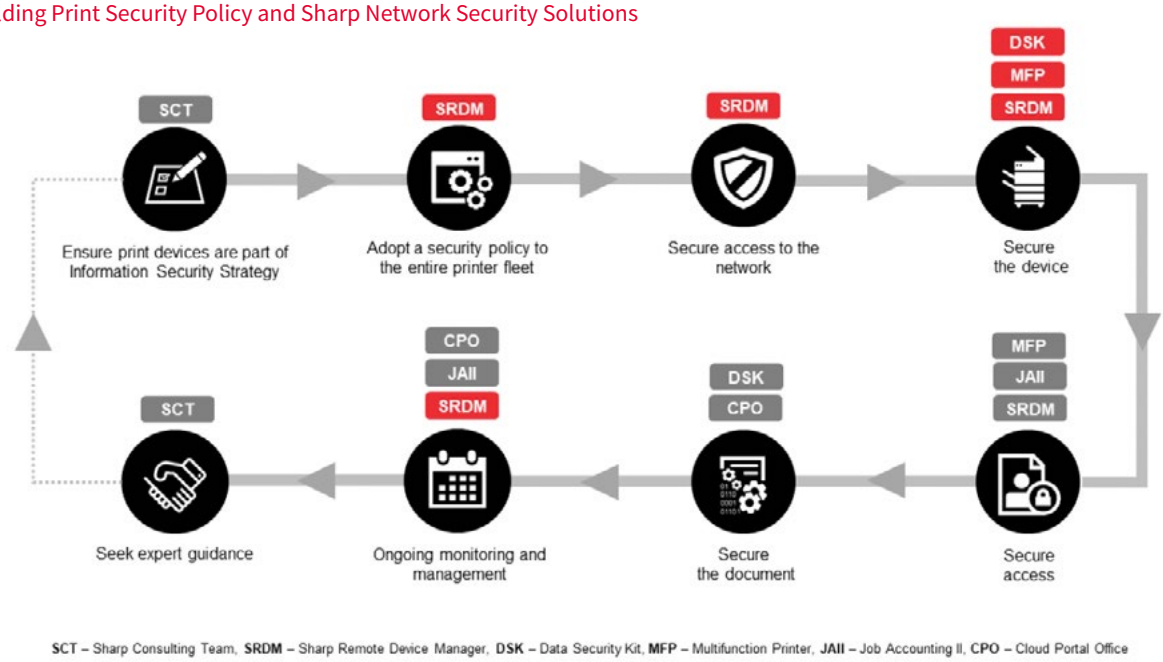
Security Package

This combines a Customer Workshop and Sharp Remote Device Manager installation and optional Output Management system configuration and deployment to cover more of the office security – Network Security & Output Security.

Sharp Remote Device Manager (SRDM)

This Sharp tool helps you implement critical security settings within seconds. The implementation is delivered as a service by a trained Sharp team. Based on your needs and requirements, all relevant security settings will be introduced to your IT environment and all Sharp MFPs and Printers will be under control.

Building Print Security Policy and Sharp Network 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

So what have we learnt? The good news is that it's not all bad news!

While MFPs and Printers certainly represent a serious (and currently underestimated) threat to businesses there are some clear steps that you can take to mitigate the risk.

- You are not alone – threats are everywhere. Every day we can find information on data breaches, cyber-attacks, viruses and other malicious activity on businesses of all sizes. The most important thing is to understand how your business could be affected if it was attacked and ask the question 'Is my business really prepared to defend itself?"
- The solution is not always simple. To understand, configure and execute appropriate security measures and functions can take ages and cause real implementation difficulties. As every organisation is different, you need to apply different tools and introduce unique strategies that tackle the specific threats to your business. But, whatever your particular needs, Sharp can help you create an effective security solution to safeguard your MFPs and Printers.
- If your business is not prepared, try to understand the problem. Why is your business vulnerable? Does it have sufficient tools and resource to introduce or enhance your Network and Print Security Policy? Or should you use Sharp specialists to audit your networks and network peripherals and introduce relevant security tools to your business.
- Set up your own security goals. In order to understand your potential vulnerabilities and what you need to protect you need to answer the questions "Where should my organisation be in a few years from now" and "How can I prepare my business to take the necessary steps needed to introduce the appropriate measures and tools to prevent cyber attacks, malware, etc. in the future".
- Ensure you have the right expertise. If you have the necessary in-house resources you can build your own Print Security Policy. Or you can use the Sharp Professional Services team to help build an effective security system and introduce tools relevant to your business type and needs, including:
  - Sharp secure network devices, which are compatible with the latest security certificates
  - Sharp security software, solutions and services that help build a Print Security Policy: DSK, SRDM, Print Security Audit, etc.
- We are here to help. We can ensure that you don't suffer from unexpected delays in your Print Security Policy review and implementation. Sharp representatives are ready to help you understand your current business security level, review it, and propose a strategy that will deliver a consistent Print Security Policy that suits your organisation's need and requirements.

Our specialist will help you choose the relevant tools and services from the following:

- Sharp Standard Security features
- Optional tools, e.g. SRDM
- Optional enhancements, e.g. DSK
- Sharp Network Security Package
- Sharp Security Audit
- Print Security Policy.

- Always consider the bigger picture. To avoid potential vulnerabilities in other areas of your organisation, we can help you introduce further security measures from the Sharp portfolio so that you can deliver 360-degree security protection for every aspect of your business:
  - Network Security
  - Output Security
  - Document Security
  - GDPR compliance

Sharp Security Framework

You can find out more about all of our security solutions 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. Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years. R*eport, IDC, Q4 2018*

2. IT and Print Security Survey 2015. *IDC, September 2015*

3. Printing: a false sense of security. *Quocirca, 2013*

4. Transformative Technology in Document Security. *IDC, May 2015*