brother
at your side

Brother Security White Paper

April 2016

THE HIDDEN THREATS POSED BY YOUR PRINTER

(AND WHAT YOU CAN DO ABOUT THEM)

Printer and scanner setups in businesses and other organisations are increasingly versatile and powerful. But with these advances comes greater security risks, and very few organisations are taking sufficient steps to protect themselves.

Security measures at work are a familiar part of most of our daily lives. Everything from ID cards or keys to control physical access, to using network security software to protect access to information, are used routinely by organisations to protect their assets. Even the idea of having an email account without a password seems completely reckless.

But there is one area in which many organisations still have potential security weaknesses – the way IT equipment such as printers or scanners connect to their otherwise secure network.

In a 2015 survey, Brother asked over 2,500 SMBs about challenges to their business. 75% said they felt that information security is very important to their organisation, and 59% agreed that information security impacts decisions around printing and document management.

These attitudes and concerns are rising in tandem with – and in response to – a rising number of security issues across sectors. A Quocirca study of 200 enterprises also conducted in 2015 revealed for the first year, security has risen to the top of the agenda with 75% indicating that this was an important or very important driver (average score of 4.01 out of 5). Overall 74% of organisations have deployed are or planning to implement secure print solutions.

So what exactly are the threats?

Essentially, there are four ways in which networked printers or scanners can pose a threat to an organisation.

1. **BY ACCIDENTALLY LEAKING CONFIDENTIAL PRINTED INFORMATION**
2. **BY ACCIDENTALLY LEAKING CONFIDENTIAL SCANNED INFORMATION**
3. **BY ALLOWING NETWORK INTRUSIONS THROUGH LOWERED SECURITY**
4. **BY ALLOWING UNAUTHORISED USERS PHYSICAL ACCESS TO UNGUARDED DEVICES**

To help organisations eliminate these common security threats, Brother have outlined the specific risks administrators should be aware of, and the kind of purpose-built technology that can be integrated with existing security for better protection.

1. ACCIDENTAL LEAKAGE OF CONFIDENTIAL PRINTED INFORMATION

What are the dangers?

It doesn't matter how effective your organisation's security policy is - if someone can walk up to a printer, pick up uncollected pages, then walk away with them then your data is at risk.

Most of us don't sit right next to the printer we use, so there's always a risk that uncollected print jobs – potentially highly sensitive documents - can be left exposed to anyone walking past them.

What can organisations do about it?

The only way to effectively combat this issue is to delay printing until the authorised user is at the machine, and the best way to do that is with a PIN or secure card reader. Depending on the size of the organisation and its requirements, Brother recommend several different solutions. The first is **Secure Print**, a feature primarily designed for people who only occasionally print confidential documents. Secure Print allows users to delay the actual printing process until they are physically in front of the printer. Therefore, if you find you need to print something sensitive, you simply assign a PIN number to that job in the driver as you're sending it to the device. If you print confidential documents on a more regular basis, something like **Active Directory Secure Print** will be more effective. This feature totally restricts physical access to any function on the printer by essentially locking out any unauthorised persons. To unlock the printer and collect your document, users first authenticate themselves using their existing Windows® Active Directory username and password. In both cases the job is stored to the printer's internal memory until it's collected.

To use Active Directory Secure Print an organisation needs to already be using Microsoft® Active Directory, but for organisations that don't, Brother also supports secure printing to LDAP supported user database servers. This works in the same way as Active Directory Secure Print, but communicates with an LDAP enabled server.

For an extra layer of security using either Active Directory or LDAP secure print functions, administrators can specify a time limit for how long uncollected print jobs can remain in the devices memory. So confidential documents don't remain indefinitely inside the machine.

For environments where the need to print confidential information varies for different users, a more network based approach is likely to be more suitable. Something like Brother's PrintSmart Secure Pro stores the documents on a central server instead of the device. This means users can collect documents from any printer in the building that's connected to the PrintSmart Secure Pro server using their PIN or, where supported NFC Cards authentication, and administrators can monitor usage more closely too.

Even with those measures in place, there is still a weakpoint – with the right software your data can be intercepted as it travels to the printer itself. To safeguard against this, Brother devices have built in Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption, the same technology used in e-commerce to protect bank and credit card details. So your most confidential files can be encrypted at up to 256-bit during transmission over the network.

2. ACCIDENTAL LEAKAGE OF CONFIDENTIAL SCANNED INFORMATION

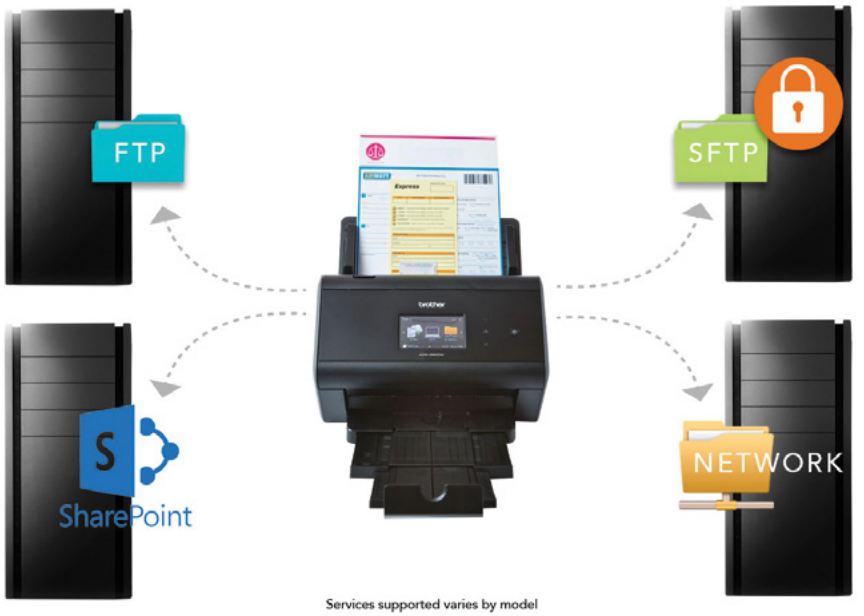
What are the dangers?

Even if your printer is secure, there is still another potential leak risk not too far away: through your scanned documents. Once a confidential document has been scanned, there are many options open to the user on how to store or share it. Sharing scanned documents by email or uploading to them to the web are highly risky strategies with sensitive data, since documents can reach unwanted eyes so quickly with a relatively small mistake. Worst still, there are no limits to the number of copies that could be made.

What can organisations do about it?

The simplest solution is to turn your scanned document into a PIN protected **Secure PDF**. Brother's single / multifunction scanners can all instantly secure any new PDF file with a four digit PIN, so nobody can open it without your permission.

Alternatively you can use many Brother single and multifunction scanners to **Scan to SFTP**. Secure File Transfer Protocol establishes a private and safe data stream, and by controlling access to SFTP servers more closely, organisations can actually help keep the whole network even more secure by closing fully a gateway in and out of their system.



3. POSSIBLE NETWORK INTRUSIONS THROUGH LOWERED SECURITY

What are the dangers?

It's standard practice to expect tablets and laptops to require certificates, usernames and passwords when joining a secure network. But many generally don't expect printers to do the same, even though their point of connectivity can present just as much of a threat to the security of the overall network.

What can organisations do about it?

External threats

Because their devices have various types of built-in encryption, Brother can suggest a number of ways to improve security and plug the gap.

802.1x: Brother devices all conform to the very high security standards set by IEEE under 802.1x rules, whether they are hardwired with a cable or part of an organisation's wireless infrastructure.

IPsec: multiple Brother devices can be connected directly to internal or external secure environments using IPsec, saving time, money and effort. Because they come with IPsec built in, there's no need to install middleware or use third party hardware to connect both end-points together.

SNMPv3: Designed to comply with strict network security policies, Brother devices understand all instructions given to them in encrypted SNMP versions 1, 2 & 3 (MD5 and SHA1), even during remote setup and routine maintenance.

Even if organisations are using their own print fleet management tool instead of the Brother BRAdmin utility to centrally manage their devices, Brother printers will still integrate into their secure networks quickly and easily.

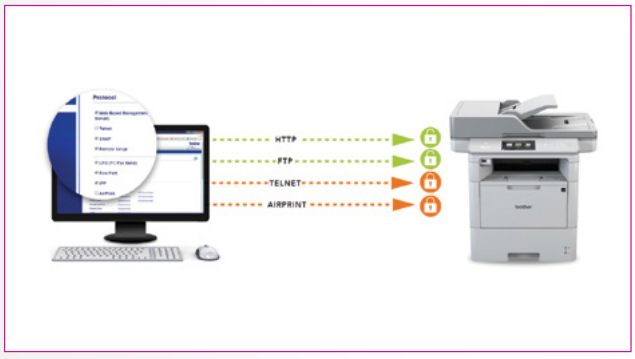
Internal threats

While encryption protects agains external threats, If internal staff members can remotely access network-connected printers the network can be vulnerable. To prevent any issues leading from this, Brother printers support **Password Protected Embedded Web Servers**, which will time-out after a period of five minutes of inactivity.

They also support **IP Blocking**, which will prevent access to the device over the network. In this example, the printer will only accept connections from users with the following IP Addresses: 10.45.12.1, 12.45.12.45, 10.45.12.46 & 10.45.12.47

For a less restrictive solution, **Protocol Control** allows administrators to disable protocols that aren't required without completely blocking access to everything, such as FTP or SMTP.

The example below shows how an IT administrator has disabled the following functions: Telnet, AirPrint, Proxy & FTP Server. For a less restrictive solution, Protocol Control allows administrators to disable protocols that aren't required without completely blocking access to everything, such as FTP or SMTP. The example below shows how an IT administrator has disabled the following functions: Telnet, AirPrint, Proxy & FTP Server.



4. UNAUTHORISED PHYSICAL ACCESS TO UNGUARDED DEVICES

What are the dangers?

Despite having all these security rich features, unless printers are physically locked away in secure rooms, people can still walk up to them and attempt to retrieve data from them. For small to medium businesses with little or no IT infrastructure, some form of physical security is especially important.

In Brother's 2015 study, two thirds of decision makers said that information security impacts on their printing and document management decisions, among their concerns being the way that documents are held by the printer.

What can organisations do about it?

For those organisations, Brother devices have a range of secure functions that will prevent authauthorised people from tampering with them.

Setting Lock does what you would expect – it restricts access to the device's settings through its control panel. This is ideal for organisations that don't want to limit the way people use the functionality but that do want to make sure unauthorised users can't change any settings.

Secure Function Lock takes that one stage further by preventing access to both the device's settings and certain functions. This allows administrators to decide who can do what with each machine, for instance controlling which users are able to fax and scan, or imposing monthly limits, through unique PIN numbers or NFC access cards.

The screenshot below is from the Secure Function Lock settings page from the device's embedded web server. It shows that all functions are blocked to unauthorised users. This is shown in the first row called Public Mode. User 1, as shown in the second row has unrestricted access to all functions.

User 2, as shown in the second row does not have the ability to send or receive faxes and has a 100 pages print limit. This limit can be manually adjusted and reset by an administrator or set to reset on a cyclical basis.

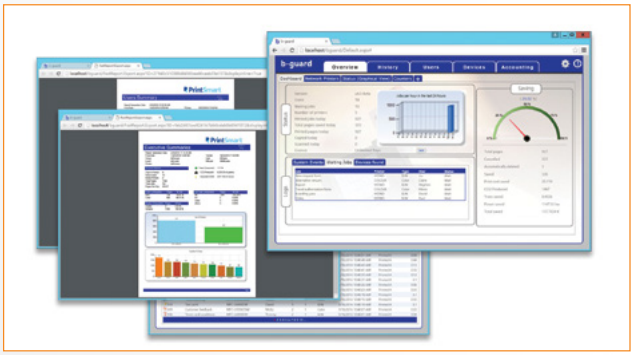
In cases where organisations share printers between multiple users or need to put them in public places, controlling abuse without obstructing normal use can be difficult. But with Brother's Active Directory or LDAP authentication staff can easily use their existing network login credentials to gain access to printers on the go.

The Whole Package

For organisations that know they want to control their security and see in more detail how their devices are being used, Brother offers **PrintSmart Secure Pro**, an innovative and affordable software solution that increases security, improves efficiency, makes print costs visible and reduces paper wastage, aiding the environment. A simple user interface gives IT administrators greater control, revealing all they need to know about their company's print usage, enabling them to manage and monitor activity and track, control and reduce print costs.

Brother printers can also integrate into third party print management solutions through their open interface. **Brother Solutions Interface (BSI)** is an open interface platform designed to let third parties create their own solutions for Brother devices.

So, rather than being tied to a pre-determined approach, organisations can customise the User Interface to whatever they want.



Recommendations

There's no doubt that many organisations across every sector need to take the security threats posed by printers and scanners to their data and network more seriously, but there's no single solution. IT administrators need to select the appropriate solutions for their unique risks, infrastructure and existing security. But if an organisation can be sure they have:

1. **Made their devices secure**
2. **Protected their data en route and after printing**
3. **Protected their network from intrusion**

then they can feel confident that their printing and scanning systems will be well-protected against security issues in the near future.

[1]Source: Brother SMB Research conducted by B2B International among 2,502 businesses in the UK, France, Germany and USA

[2]Source: Quocirca Managed Print Services Landscape, 2015. Survey of 200 organisations with 1,000 or more employees in the UK, France, Germany and USA