Think print, think security

Plugging the printer security gap

April 2010

The widespread use of networked printers and multifunction peripherals (MFPs) which scan, print, fax, copy and email has increased productivity in the production of all types of business output. However, the growing sophistication of these devices has also increased security risks associated with printing. Network connectivity, along with hard disk and memory storage, means that MFPs are now susceptible to many of the same security risks as PCs and servers alongside the traditional risk of sensitive printed output getting into the wrong hands. However, all too often the security of the print environment is overlooked and little is done to mitigate these threats.

Although most businesses recognise the serious consequences of confidential data being leaked externally most do not realise the exposure that an unsecured printing environment introduces to their business. With printing being an essential part of many business processes, protecting network printers and MFPs should be a critical part of any organisation's IT security strategy. Printing security is paramount in three key areas: users, documents and devices. By controlling user access, protecting documents and securing devices businesses can address requirements for data confidentiality and regulatory compliance that are only set to get tougher.

Louella Fernandes
Quocirca Ltd
Tel +44 1753 754838
louella.fernandes@quocirca.com

Bob Tarzey
Quocirca Ltd
Tel +44 77900 275517
bob.tarzey@quocirca.com

1   Introduction – is printing the weak security link?

With an ever increasing number of data security breaches hitting the headlines, protecting data from both internal and external threats has become critical for businesses subject to a plethora of regulations. Unauthorised access to data can lead to an information leak or breach of confidential data - whether it is an organisation's financial information or intellectual property. It may increase the risk of identity theft or pose regulatory risks if personal data is involved. For businesses of all sizes, lost or stolen data not only exposes a business to financial penalties and legal ramifications, it can also severely tarnish its brand and reputation.

While many businesses continue to invest in information security to safeguard their IT systems from external and internal threats, few pay the same strategic attention to protecting the print infrastructure which plays a critical role in the creation, output and distribution of documents. Without proper controls on printing devices, business critical documents can be routed in seconds to unauthorised individuals.

Printers are easy to overlook when evaluating IT security, as they are often considered as "dumb" peripheral devices. But gone are the days of securing a printer by placing it behind a locked door. The latest evolution of multifunction peripherals (MFPs) and network printers are integral to today's office environments. But while shared printers have brought speed and convenience to the office, they have also introduced security threats that many IT departments have not adequately mitigated. With the capability to print, copy, scan to network destinations, store on local disk drives, send as email attachments and handle incoming and outgoing fax transmissions, MFPs have many of the characteristics and security vulnerabilities of any server on the network. Even standalone, these "intelligent" devices retain latent document images, potentially exposing sensitive information. Hard disk storage, multiple network ports open to all users, powerful processors running embedded operating systems, web servers and email clients mean that an MFP is anything but a dumb device.

As printers are commonly located in communal areas with only basic physical security, it is very easy for printed information to end up in the wrong hands, either accidentally or intentionally. And if an MFP has the ability to email scanned documents without security measures, it could be used to forward confidential documents outside the company with no way of tracing the sender.

Almost all organisations produce printed data that would be damaging to some degree if compromised or abused. Think of the type of documents that are printed, copied, emailed, faxed or scanned on a daily basis - personal information, financial statements, confidential reports, emails, customer data and employee information - inadequate protection of printing devices can have serious implications. There are many cases where the confidentiality and integrity of information has been compromised. In 2007, an employee of an investment branch of a large bank was arrested in New York. He was seated by a shared printer, and read what his colleagues were printing. Amongst this information was data about upcoming mergers and investment decisions. The employee had forwarded that information via email and mobile phone; his accomplices then bought and sold shares, making around $7M with the scheme. The bank was fined for insider trading and the employee sent to prison for several years.

Of course, guarding against security breaches isn't the only security challenge organisations face today. Companies must also closely safeguard their data to be compliant with a growing list of government and industry regulations, which include Basel II, MiFID and the Data Protection Directive in Europe. A common characteristic among all of these laws is the requirement that organisations control access to data, audit how it is being used, manage its distribution, and shield it from loss or unauthorised changes.

Many businesses never consider the potential risks associated with an unsecured print environment, but it is possible to use devices safely by establishing a security strategy that protects networked printers and MFPs. Quocirca believes that businesses must extend their IT security and compliance strategy to include printing. Businesses must adopt a layered approach to print security, which encompasses introducing security approaches as close to the point of creation as possible, bolstered by enabling built-in printing security features, implementing advanced secure printing solutions where required and including best printing practices in information security policies. Nevertheless, the effectiveness of an organisation's security strategy is only as strong as the weakest link. To minimise the exposure, a balance must be struck between people, process and technology – for example, secure printing technology can minimise the likelihood of confidential

printed output remaining unclaimed, but cannot eliminate the possibility of sensitive documents left in a waste bin through employee error.

This paper highlights the key security vulnerabilities of networked printers and MFPs and discusses the techniques that can be used to mitigate these risks. This paper should be read by anyone who has responsibility for IT security or the management of printers.

2   Where are the vulnerabilities?

Key Findings:
- With hard disks, memory and embedded software, networked printers and MFPs are vulnerable to network-based attacks and data security threats
- Devices often feature embedded web servers, and run more vulnerable services than networked PCs
- Few businesses are aware of the threats of operating an unsecure print environment

Shared networked printers and MFPs are open to both data and network security threats. As the move to consolidation around MFPs continues, today's printers are less commonly used as purely personal devices. Whilst we are all familiar with the "print and sprint" dash to the printer once confidential or sensitive material has been sent, this is only one security vulnerability amongst many more, as shown in Figure 1.
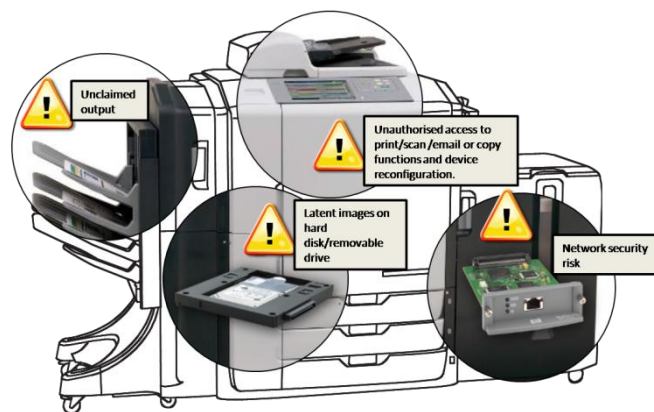

Figure 1. MFP Security Vulnerabilities

Printing security threats can be broadly split into the following categories:

At the device:
- **Unclaimed output.** A user with unrestricted access to the printer may take a confidential document printed by someone else. Vulnerable documents include printed or copied items left inadvertently on the printer output trays and received faxes sitting unattended on a MFP. Such documents can easily end up disposed in ordinary waste
- **Hard disk and memory:** The hard drive stores various types of hardcopy information such as user information, copy/scan/fax/print images from processed jobs and device logs. Without security or logging measures, unauthorised users may be able to store and retrieve files. Equally, if the drive were to be removed, it could be connected to any PC and the data analysed.
- **Scan-to-email functionality**. Without authentication it is possible for users to enter source and destination emails. This means confidential information can easily be distributed to the outside via scan-to-email or fax transmissions, without trace of the sender's details.
- **Firmware:** Data can be intercepted and sent to a third party using a number of methods. Firmware on some printers could be modified to add this ability or other special features such as a network sniffer. This could be done by either uploading modified firmware or by modifying and replacing a chip on the printer's circuit board.

On the network:

- **Denial of service attacks:** Any device with a network interface could be susceptible to a denial of service. Tampering with device administrator settings or changing the network location of the printer removes the document output system from operation or makes it otherwise inaccessible, thereby preventing users from being able to output documents.
- **Open or unused ports:** An external hacking attack could be launched through unused or open ports.
- **Accessing print jobs in print queues:** It is possible to steal documents in queues or in local memory. Also, general network information can be hijacked by simply looking at the configuration settings of an unsecured printer's network and enabling attacks on other network devices

For any business that fails to protect its data assets, the implications can be serious - including damaged reputation, financial penalties and ultimately lost customers and revenue. Securing the print environment should therefore be a vital part of an overall security strategy to ensure a business can more fully protect its assets, employees, customers and ultimately reputation. Fortunately there are ways to mitigate these risks through using a print device's built-in security features or by implementing new or modifying existing document security measures.

3   Mitigating the risk

Key Findings:
- Document security begins at the point of creation
- Print security protects and monitors access to printers, through built-in security capabilities and advanced tools
- Many printers are equipped with a variety of features that can be used for network security such as SNMP v3, IPSec, HTTPs and user and network authentication
- Advanced security features include hard drive erase, encryption and tools for auditing usage.

To guard against the potential threats of an unsecured print environment, there are a variety of measures that can be taken that complement the built-in security features of many printers and multifunction devices. These capabilities minimise the risk of unauthorised access to documents, guard against hacking and other network-based security threats and audit user activity.

3.1 Start at the point of creation

The use of automated classification tools makes the handling of information easier. For example, documents created that are marked as "public" or "open" can be printed without any issue. Those marked as "private", "classified" or "top secret" may need to be dealt with in different ways. Rules-based engines can then be used to ensure that different styles of documents can only be sent to certain print devices, for example, "classified" and "top secret" only being able to be printed to a secured printer in a trusted environment.

Data leak prevention (DLP) tools can also help. Here, the actual content of a stream is looked at, and if certain content is found within it (either as a direct one-for-one comparison of text blocks or as a "close enough" comparison using intelligent algorithms), the print job can be automatically blocked, re-directed or a message provided to the user to ensure that they are aware of the risks involved in sending such a job to the specific print device.

3.2 Taking print precautions

Classification and DLP, however, will not provide the full levels of security needed. Organisations can adopt some or all of the following features depending on their individual business needs. To provide complete protection of information that is captured and produced by printing devices businesses should take the following precautions:

Secure the physical device

- **User authentication.** MFP functions can be restricted so users must authenticate prior to performing copy, scan to email, scan to fax, scan to network, workflow scripts or embedded applications. MFPs

can be configured to authenticate users against the organisation's corporate directory via LDAP, LDAP over SSL or Kerberos for instance. These authentication methods are secure and are generally compatible with Microsoft Active Directory and other directory servers. This means that if a user sends an email from an MFP, the user's email address is automatically inserted, meaning the resulting email is not anonymous or attributable to anyone else. Authentication also enables auditing and the application of any print policy which enforces what different functions users can perform.

- **Print jam recovery.** Use features to prevent a printer automatically reprinting jobs after a paper jam is cleared. Often, the originator of a print job is not the person who clears the jam, and it is unlikely that whoever does clear the jam will try and identify the owner of the document or documents that then come out from the printer. This feature is often available on print management tools or installed drivers.

- **Hard disk erase.** For organisations that require a higher level of protection, encryption and data erase capabilities protect all temporary data and stored documents on hard disk drives. Encryption standards include 256-bit AES (Advanced Encryption Standard) or 168-bit TDEA (Triple Data Encryption Algorithm). Data Erase features can be configured to overwrite once with null data, overwrite once with random data, or overwrite with random data three times for maximum security. When data has been erased it is effectively permanently irretrievable. Disk erase enables administrators to clean the drive, and also enables the device to be wiped clean for security if recycled or resold. Businesses should determine if encryption is required based on the type of documents most commonly printed.

Secure the network

- **Disable unused network ports and protocols.** Keeping unused ports and protocols open invites unauthorized access and threats from hackers. For this reason, it is advisable to keep unused ports and protocols closed. For example, in a network using only TCP/IP, close protocols such as Ethertalk, Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), and so on.

- **IPSec protection.** For printers and MFPs, IPSec is used to protect print job data sent between a host and the printing device. By applying IPSec between the printer and host, data between these systems can be secured with strong encryption. This protects the content of print jobs from network eavesdropping.

- **Network authentication with per-user authorisation for individual services.** Customised access to individual services such as Scan to email can be set up to require user authentication at the device. Authentication can require a device-based password or be seamlessly integrated into an IT environment via a central directory server.

Secure user access

User authentication and access control features help to secure user access and also audit user activity.

- **Pull printing.** This addresses the basic concern of printed pages lying on the printer for anyone to pick up. With pull printing, the printer holds submitted jobs until the intended recipient is present at the device. By producing the printed job only when smart card authentication or the proper PIN code is entered on the printer's operator panel, the job is delivered securely into the right hands. Unprinted jobs can be automatically purged after specified amount of time, to avoid a build up of old jobs.

- **Operator panel lock.** Printer or MFP device configuration settings can be accessed from the front panel of the device by pressing the Menu button. This ease of use can lead to non-administrators accessing configuration settings and making unwanted changes. To minimise the risk of non-administrators gaining access to the configuration settings, administrators can lock the control panel through password protection.

- **Usage auditing.** Auditing tools which monitor print history and usage enable IT managers to track all printing activity on their devices. Access to and utilisation of copy/print/fax/scan by user or group helps prevent unauthorised use.

3.3 Benefits beyond security

The benefits of securing networked printers and MFPs are manifold, and extend beyond security. Businesses can also cut costs and reduce waste by carefully managing usage through centralised print management tools.

- **Increased confidentiality and compliance.** Follow me or secure release solutions make it easier to keep confidential materials out of the wrong hands. Audit and tracking capabilities enable full traceability of print jobs helping meet requirements for audits against data protection standards such as ISO 27002 or PCI DSS.
- **Reduced costs.** Monitoring and logging printing activity so that adjustments can be made on an ongoing basis, driving optimisation and allowing users to do what they need to without the ability to abuse resources will enable considerable cost savings. Enforcement of central controls can also limit the use of personal printing on office devices by, for example, assigning user printing quotas, so making users think more before printing unnecessary jobs. Minimising unclaimed printing and adding accountability reduces paper waste, toner and energy usage as it encourages users to print only the documents they actually need.
- **Enhanced user productivity.** Secure solutions mean that users can securely release print jobs at any device by either PIN or smart card authentication. This promotes mobility by allowing users to release documents at any convenient printer, anywhere in the organisation avoiding the inconvenience of printers that are busy or out of service.

4 Industry standards for print security

The security requirements for printing are highlighted by developments such as the IEEE P2600 hardcopy security standard working group, ongoing introduction of security-focused products, and manufacturers' efforts to gain security certifications for their output devices. The most important standards with regard to printing are:

- **Common Criteria certification**

The Common Criteria (ISO 15408) is a standard for computing security, which can also be applied to document output devices. Some device manufacturers have certified their equipment under the Common Criteria process. But because of the process's cost and complexity, certification is often limited in scope to a subset of device functionality – such as hard disk overwrite capability.

- **IEEE P2600**

The IEEE P2600 working group is defining a security standard for hardcopy devices, as well as recommendations for the security capabilities of devices when deployed in various environments, including enterprise, high-security, small office/home office, and public spaces. The p2600 working group has broad industry participation, including Hewlett-Packard, Lexmark, Canon, Xerox, Sharp, Ricoh, IBM, Epson, Okidata, Equitrac, and Océ

- **ICSA Labs NAPS certification**

ICSA Labs, an independent division of Verizon Business, announced the NAPS certification program in September 2009. This includes rigorous testing that examines several different aspects of a networked printer and copier device and how each impacts its overall security. ISCA is also hoping to gain attention from enterprise clients concerned about device security with a NAPS assessment program that offers an evaluation and report with results of testing and recommended configuration instructions.

- **National Institute of Standards and Technology (NIST) Security Checklist**

The National Institute of Standards and Technologies (NIST) have been tasked by U.S. legislation to develop checklists that facilitate security configuration of devices likely to be used by the U.S. Federal Government. NIST has requested IT equipment manufacturers to develop these security checklists for their products. Details of the checklist program are available at http://csrc.nist.gov/checklists. NIST will review manufacturer's checklists for relevance and correctness and publish those checklists on a searchable NIST website.

While certification may be useful in confirming the manufacturer's claims of functionality, it is not sufficient in itself for the implementation of a secure printing infrastructure. As there is no industry standard that a printer manufacturer must certify against, each manufacturer chooses which security features it considers to be important and certifies only those features. Therefore businesses should evaluate the standard and optional security mechanisms on devices such as image overwrite, authenticate, removable hard drive, hard drive erasure and basic access authentication as well as considering third party secure printing solutions from companies such as Safecom or Ringdale.

5   HP case study - Allied Irish Bank (AIB) deploys security measures as part of an HP managed print service (MPS)

AIB Group is the leading Irish financial service provider, and offers a wide range of personal banking services including loans, credit cards, mortgages and general insurance products. It comprises four divisions; AIB Bank ROI, AIB Bank UK, AIB Capital Markets and AIB Poland. AIB Bank ROI, AIB Bank UK and AIB in Poland through its 70.5 per cent holding in BZ WBK provide retail and commercial banking services to their respective countries whilst Capital Markets manages investment banking, asset management, corporate banking and global treasury activities.

Business challenge

AIB wanted a Managed Print Services (MPS) solution at its head office that would improve service quality, deliver cost savings and lower operational risk. Its printer, copier and fax fleet had evolved to a ratio of 1 device for every 4 employees in its Dublin's Head Office locations. The print environment comprised multiple vendors and multiple contracts without any true ownership for print - it was divided amongst many different functions. With this disparate environment AIB could not monitor costs or control its print budget.

Solution chosen

AIB chose a full HP MPS solution which standardised and consolidated the existing fleet, moving from 1 device per 4 employees to a ratio of 1 device per 12 employees. The MPS solution included SafeCom software to improve management of its print environment and enable enhanced print security to reduce operational risk. Print jobs are enabled by the use of the Staff ID card and badge readers on each device. Scheduled but unprinted print jobs are deleted automatically overnight.

Benefits gained

The optimised print infrastructure is now more easily managed and productive due to improved workflows such as the implementing of pull printing. The print environment is now highly reliable and secure with cost management under control and service quality much improved. AIB has seen a difference in the way its employees manage document workflows throughout the company. The use of scan features has led to more efficient printing practices as well as a reduction in paper wastage.

Overall the use of MPS to consolidate the hardware fleet has led to projected cost savings of 20 to 30 per cent and a predicted 50 per cent reduction in AIB's carbon footprint of the printing facilities at its head office, reinforcing the bank's environmental policy.

Source: HP MPS case study authorised by AIB

6   Recommendations

So what can businesses do to narrow or close today's print security gap? Quocirca recommends the following steps:

- **Establish a secure printing strategy and include the printing environment in the overall security strategy of your organisation.** Ensure that the secure print strategy considers polices, standards and procedures along with technology, resource requirements and training. Different organisations have different security requirements, so adopt a layered approach that begins with basic protection and can be enhanced with advanced capabilities as business needs change.
- **Integrate with broader IT security** – Data classification, data loss prevention (DLP) and end point security tools are used to control what users can do with data e.g. copying, sending by email – make sure the policies that control these define who can print what. DLP can prevent a file being sent to the printer based on the content of the file, many tools actually scanning down to the sentence level, for instance "*this document cannot be printed under any circumstances*" or "*this document can only be printed on a secure printer*".
- **Use trusted advisors for needed expertise**. Trusted advisors such as IT consultants or resellers with security specialism can help businesses match their print security needs with appropriate solutions. This is especially important when reduced staffing is an issue.
- **Gain control of printer fleet.** Businesses should think about which print security features are needed and look for devices with built-in capabilities, or ensure existing devices support the required security features.

Firmware should be continually monitored to install updates that fix existing security concerns and add new features. Device consolidation helps reduce reliance on older print technology and also ensures that the optimised infrastructure can be centrally managed and monitored.

- **Use layered security**. Employ the level of security specific to business and industry need. Although all business should protect personal and customer data, the level of compliance varies depending on sector with, for example, legal, medical and HR requiring high levels of security and confidentiality for documents. Consider a layered approach deployment that encompasses pull printing, hard disk erase or encryption and auditing tools. Implement a full audit/tracking mechanism for printed jobs especially for organisations where service users (e.g. customers, students and other third party) may regularly use networked printing resources.

- **Don't forget printer disposal.** Network printers have to be disposed securely, in terms of any sensitive or confidential data that may reside on hard drives or memory. Use software to scrub all hard drives and flash memory to ensure data can't be recovered. Vendor and third-party tools offer disk erasure that meets industry and government regulatory requirements, such as the UK's Waste Electrical and Electronic Equipment (WEEE) directive. For even more rigorous data removal, consider degaussing (demagnetising) and even physically destroying hard drives and memory.

- **End user training**. Promote awareness of good printing practices and how a controlled printing environment can increase corporate security levels, user productivity and reduce costs.

- **Regularly monitor and test the print infrastructure.** By tracking and monitoring usage and access to printing resources unusual behaviour and anomalies can be alerted and can potentially prevent a breach. Determining the cause of a printer security breach is impossible without user activity logs.

7   Conclusion

Printer security is a complex issue with many elements to consider. Failure to take steps to protect information assets can have serious consequences and risks exposing an organisation to liability claims, financial loss and criminal penalties. Whether it is personal or financial information, health records, confidential government information or sensitive corporate data it is vital to deploy security that minimises the risk of targeted or opportunistic threats - be these internal or external.

Ensuring a secure printing environment is critical for any organisation regardless of its size and maturity. It is therefore imperative that IT managers prepare themselves and their organisations to manage print in a proactive way and implement policies and procedures to support an overall secure print strategy. It is not simply enough to throw technology at the problem, as the effectiveness of any security strategy relies on user education and improved processes. For security and compliance, businesses need to identify who uses printing devices, control how they are able to use them and gather accurate usage audits for reports to regulators. In today's digital world, minimising security risk and protecting confidential information has become a top priority and protecting network printers is a critical part of the information security equation.

About HP

HP, the world's largest technology company, simplifies the technology experience for consumers and businesses with a portfolio that spans printing, personal computing, software, services and IT infrastructure. More information about HP (NYSE: HPQ) is available at http://www.hp.com/.

quocirca

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com