Effective print security for SMBs

_Increasing printer fleet security and document confidentiality_

October 2012

Businesses of all sizes have data of value, such as employee and customer information, which must be protected. While many businesses have secured their IT infrastructure to minimise unauthorised access to confidential or sensitive data, unsecured MFPs and networked printers remain a critical source of vulnerability.

Network connectivity, along with hard disk and memory storage, means networked printers and multifunction peripherals (MFPs) are susceptible to the same security risks as any networked device. Without proper control, it is all too easy for sensitive or confidential information to fall into the wrong hands.

While SMBs face challenges around data protection and compliance, they also grapple with resource and time constraints. Consequently, they often mistakenly downplay the importance of print security.

This paper highlights the risks of unsecured printing and discusses how integrated print management provides SMBs with a simple and scalable approach for print security.
Introduction

Many small to mid-sized businesses (SMBs) continue to have a heavy reliance on printing to support business activities, particularly in the legal, financial and healthcare sectors. However, this reliance can come at a cost. Whilst networked printers and MFPs have enabled high productivity in the workplace, they can easily be compromised if not adequately secured. The consequences of inadequate protection could be bad publicity, financial loss, identity theft, risk to intellectual property, or even fines and criminal charges in the most severe cases.

SMBs are often at greater risk of their employees mishandling data than larger enterprises, according to a recent Ponemon Institute report\(^1\), and these threats are becoming more prevalent because of the mobility of the workforce and consumerisation of IT.

Meanwhile, the Ponemon Institute’s 2011 Cost of Data Breach Study\(^2\) revealed that negligent insiders were the top source of data breaches in 2011. In the UK alone, it is estimated that the average cost per record lost has increased from £47 in 2007 to £79 in 2011.

![Pie chart showing percentage of printing importance](image)

Figure 1. How important is printing to your business?

Clearly, the financial consequences of a data breach are significant, especially for an SMB. The costs are set to become even higher as the European Commission pushes for the powers to fine businesses up to five per cent of their annual turnover for data leaks that can be shown to have been the result of foreseeable negligence.

Printed output can be one of the least secure mediums, and data breaches through printed output are all too commonplace. In December 2011, a UK county council was fined £130,000 for mistakenly sending out personal information to the wrong recipient after an employee inadvertently picked up the wrong report from a shared printer. This is not an isolated incident - Quocirca’s 2011 Enterprise Print Security study\(^3\) revealed that 70% of organisations have experienced one or more accidental breaches through printed output, with 46% indicating malicious data breaches.

In Quocirca’s SMB survey\(^4\) just 41% of respondents indicated that they are concerned with the security of printed documents. This means many SMBs mistakenly assume that printers or MFPs do not need protection and so downplay the importance of print security.

This complacency is misplaced. Networked printers and MFPs are advanced complex devices with integrated sophisticated document processing capabilities allowing users to print, copy and scan to network destinations, send email attachments and handle incoming and outgoing fax transmissions, often directly from a user’s PC. With built-in hard disk drives and memory, these devices have many of the characteristics and security vulnerabilities of any networked device. Given that employees are often behind many data compromises\(^5\), along with the fact that SMBs are processing more valuable information than ever before, it becomes increasingly vital that this information is protected when it is copied, printed, scanned or faxed.

This paper highlights the potential vulnerabilities of unsecured printers and MFPs and discusses how cost-effective approaches, such as a print management solution, can help SMBs safeguard their print environment. The paper draws on research carried out by Quocirca amongst 150 SMBs with 50–500 employees in the UK, France and Germany.
The need for print security

SMBs face the same security risks as their enterprise counterparts – just because a business is small doesn’t mean it is immune to security threats and the impact of stolen data. Indeed, many SMBs are now an important part of an extended ‘value chain’ consisting of themselves along with larger suppliers and customers – and these larger organisations are increasingly demanding that the SMB exhibit the same levels of information security as they have. Two of the biggest security challenges that SMBs face today are adherence to regulatory compliance and protection of sensitive data, documents and personally identifiable information. A data security breach has far-reaching consequences that can lead to brand damage, financial penalties, legal costs and customer attrition. Over 70% of respondents in Quocirca’s Enterprise Print Security study\(^1\) indicated the security of personal data as a top concern that will drive print security adoption in the future (Figure 2).

![Figure 2](image-url)

**Figure 2.** Which of the following concerns will drive investment in print security over the next two years?

Governance, risk and compliance (GRC) requirements have put additional burdens on IT groups within retailers, healthcare providers, financial services companies, and numerous other vertical industries. Evidence is now required to demonstrate proof of data controls against industry regulations such as Sarbanes-Oxley, PCI DSS, ISO 27001/2, MiFID and the UK Data Protection Act. In the UK, the Information Commissioner’s Office (ICO) now has powers to fine companies and organisations up to £500,000 for serious breaches of data protection principles under the Data Protection Act.

Meanwhile, the growth in enterprise mobility is driving demand for employees to be able to print securely from any device (whether it is a PC or mobile device such as a smartphone or tablet) and to any printer or MFP at any location. This requires solutions that address the dual requirements of enhanced security and flexible printing across a corporate network.

### MFP security vulnerabilities

An MFP is a powerful business asset but, left unsecured, it can pose a significant threat to any business. Consider the type of documents that are printed on a daily basis – these can include personal information, financial statements, confidential reports, memos, customer, product and invoice data and employee information. Businesses are at risk from unsecured MFPs and printers that have weak access controls, unsecured management of documents and poor tracking of usage for auditing purposes.

Shared networked printers and MFPs are open to a variety of threats (Figure 3). Security vulnerabilities include:

- **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 an MFP. Such documents can easily end up disposed of in ordinary waste, so making them vulnerable to being recovered by external individuals sorting through this waste.
- **Hard disk and memory.** The hard drive stores various types of hardcopy data 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 access this store and retrieve files, either at the end of life of the device or even during general use.

- **Scan-to-email functionality.** Without authentication it is possible for users to enter any source and destination emails. This means confidential information can easily be distributed to the outside world via scan-to-email without any trace of the sender’s details, and often without a suitable log of the receiver’s details either.

---

**Figure 3. MFP security vulnerabilities**

Quocirca’s SMB study reveals a relatively low concern with the security risks of using shared printers, although 52% of larger SMBs are concerned with potential unauthorised viewing of confidential documents compared to 39% of smaller SMBs (Figure 4). In many cases this is likely to be that SMBs do not view print security as a priority and lack the budget and dedicated resources to investigate. However, the impact of an unsecured environment can be far-reaching – including unauthorised access, data theft, loss of productivity and regulatory non-compliance.
Increasing printer fleet security and document confidentiality

October 2012

Figure 4. Which would be the following concerns/objections in moving to shared printers?

Fortunately, there are a variety of approaches to mitigating these risks, depending on the level of security needed. For SMBs, one cost-effective approach is to use a print management tool that offers integrated capabilities for user access control, centralised management of devices and auditing and reporting.

Integrated print management

New print management solutions targeted at SMBs typically offer the benefits that a full enterprise solution provides, while simplifying the installation and management procedures at a lower cost. Companies that must satisfy advanced compliance requirements, as well as larger companies, need advanced features such as reporting, monitoring and tracking. However, for SMBs that do not have these requirements, strong layered print security can be implemented at economical prices.

A print management tool can help SMBs reduce printing costs, ensure document security and promote sustainable printing practices. Although print management tools vary widely in breadth and depth of features, Quocirca recommends that businesses consider the following capabilities:

- **Pull printing.** This only releases documents to authorised users, ensuring that documents are not left unclaimed in output trays. Print jobs are sent to a print server and jobs are only released upon authentication. Users can authenticate at the printer/MFP using a pin code (entered on the MFP panel) or by using a smartcard or other separate security token device. This promotes user mobility, as users can collect jobs at any printer and also frees time waiting for a printer that is busy. Pull printing not only eliminates the problem of unclaimed print jobs, but also reduces toner usage and paper costs through negating the need for users to repeat print jobs when they cannot find their original output.

- **User authentication.** This enables users to authenticate on MFPs using any built-in authentication such as LDAP, Kerberos, or Active Directory. Other authentication choices are PIN codes, proximity badges, or smartcards.

- **Unclaimed print jobs deletion.** Print jobs are given an expiration date after which they are deleted if not printed.

- **Cost recovery.** For legal, educational and other organisations using chargeback mechanisms, a print management tool can allocate print and copy costs to departments or cost centres, as required.

- **Usage limitations.** This allows administrators to control and track output at the device. With usage limitations, administrators can limit the number of copies or prints available at an account or a department level. This, in turn, provides a further level of security to complement the controlled device access, as well as the visibility to track and control costs. The use of colour duplex and/or multi-page up can also be optional restrictions when dealing with capable devices, so saving costs through optimising output for certain job types.
Increasing printer fleet security and document confidentiality

October 2012

- Audit logs and Reporting. Print, copy, fax and scan jobs can be tracked with detailed information including user, date, time, number of pages, type of paper and type of job. This enables administrators to monitor activity and control print usage and associated costs.

- Mobile printing. Some print management tools now support printing from mobile devices such as smartphones and tablets. This is typically through allowing the user to submit a document by emailing it to a pre-configured email address. The user then collects their print jobs in the same way, using an authentication method described above.

### Use case scenario: Brother b-guard in healthcare

The healthcare industry is required to manage highly sensitive and private information and there is a common need to print sensitive documents such as patient records. The increasing use of electronic records, along with advances in management, distribution, and storage of health records, also makes them vulnerable to unauthorised access.

Brother b-guard offers pull printing capabilities that allow a doctor or nurse to 'release' their print job from any chosen device in the surgery or hospital by entering a PIN code at the control panel of the machine, or swiping an ID card through an attached reader.

Any job that does not get 'pulled' is deleted based on an administrator-determined length of time (e.g. after 24hrs or 1 month).

This not only ensures document security but also can significantly reduce wastage since print jobs that are forgotten about are never printed.

---

## Print security guidelines for SMBs

One of the biggest problems that an SMB faces is, perhaps, the lack of adequate resources to invest in the best-in-class print management products. Since print security is only a part of an overall IT security strategy, it is important that the SMB implements a comprehensive, unified and easily managed print security framework.

In order to protect SMBs’ networked printers and MFPs, Quocirca recommends the following as best practices:

- **Assess your security needs.** SMBs are not immune to security threats and face increased risks to their confidential information, so safeguarding data is critical. One data breach could mean financial ruin for an SMB. Restrict employee access according to business need. Many small businesses run on trust, but internal data breaches can be a severe problem because people know the business patterns and habits and how to get around them. Know what information must be protected and understand risks and security gaps so that you can take steps to protect confidential or sensitive information. Assess risks by identifying and classifying information being dealt with in the organisation – even simply through using 'Public', 'Commercial in confidence' and 'Secret'.

- **Educate employees.** More often than not, employees are disconnected from the top management viewpoint of security. It is therefore crucial that every employee of an SMB buys into the need for print security. Develop print security guidelines and policies and educate employees about the security, cost and environmental benefits of using secure printing practices.

- **Implement integrated print management.** Implement an integrated print management solution that includes authentication, accounting and audit capabilities.

- **Evaluate the cloud.** Evaluate whether on-premise or a hosted service would best suit the managed print security needs of your organisation.

- **Business process integration.** Integrate document protection practices into business processes, particularly where those processes touch the outside world through interactions with suppliers and customers.

- **Consider a managed print service.** Managed print service (MPS) providers can help alleviate the burden for IT staff at SMBs. As few SMBs have the skills or resources to optimise and manage their print environment, using an MPS provider ensures that they can maximise the benefits of operating a managed print environment. Businesses that have adopted MPS are already addressing cost reduction imperatives, enhanced security and sustainability goals.

© Quocirca 2012
Conclusion

A print management solution that encompasses user access control, cost management and reporting features not only enhances document security, but also provides SMBs with a cost effective approach to controlling and monitoring print usage. As few SMBs have the resources or time to evaluate print management tools, they should look to other information sources, including suppliers or a trusted channel partner for advice and recommendations.

SMBs often fall prey to the same security threats as enterprises, but the repercussions are typically far worse and include decreased productivity, compliance issues, lost sales and even loss of reputation. As SMBs remain reliant on printing, they must take steps to safeguard the valuable data that is printed, copied, scanned, faxed and emailed on a daily basis. This means deploying print management tools that control user access to the device and documents. Ensuring this level of access control is not only a best practices imperative, but also a compliance imperative.

References

1 “The Human Factor in Data Protection”, a report released by Ponemon Institute and sponsored by Trend Micro
2 2011 Cost of Data Breach Study: UK, a report released by Ponemon Institute and sponsored by Symantec
3 Quocirca Enterprise Print Security study, 2011
4 Quocirca SMB printing study, 2011

Brother’s b-guard and SMB Print Management

Brother’s b-guard enables SMBs to securely and cost-effectively manage their printer fleet, offering accounting and reporting summaries to identify opportunities to save costs and increase productivity.

Pull printing: This allows the user to ‘release’ their print job from any chosen device in the organisation by entering a PIN code at the control panel of the machine, or swiping an ID card through an attached reader. Any job that does not get ‘pulled’ is deleted based on an administrator-determined length of time (e.g. from 24hrs or 1 month).

Mail2Print: b-guard enables SMBs to monitor and control printing from email-enabled mobile devices such as smartphones and tablets. Users submit a document by emailing to a pre-configured email address and then collect their print jobs following authentication at the printer.

Secure function lock

This enables the lock out of different MFP functions in order to improve device security and help save costs from the misuse of devices. For example, an SMB dealing with confidential client records can disable the scan-to-USB function to avoid sensitive documents being taken out of the business.

In addition to the basic locking of functions for all users, b-guard also enables a business to create a profile for each user or department and assign them a PIN, which can unlock the functions authorised to them. For example they may require that the accounts team be limited to mono copying and scanning whilst the marketing department has access to the full suite of device capabilities.
About Brother

The Brother Group of Nagoya, Japan, is a truly global company with offices and manufacturing plants throughout the world and products sold in over 100 countries.

b-guard – Brother’s Print Management Solution
Brother is now offering organisations a simple and cost effective solution to monitor and manage all internal printing with the new b-guard print management software. b-guard enables companies to operate more efficiently by providing greater visibility and control over printing costs, security and environmental impact – while integrating the print management for all devices (regardless of make) in one single application.

b-guard is available exclusively through Brother. For more information please visit www.brother.co.uk

Brother’s European Managed Print Service (MPS) Programme.
As the market leader in printing solutions for small and medium sized businesses, Brother brings its many years of experience to deliver a new kind of Managed Print Solution, providing a simple MPS offering that is no longer just something for the large corporate environment. It is specifically targeted to meet the output needs of small and medium businesses.

The programme is a leasing package, which includes hardware, service and supplies based on a cost per page or ‘pay per click’ basis. It includes automatic meter read collection and no minimum print volumes and supports Brother’s networked devices, including a large number of monochrome and colour laser printers and MFDs as well as A3 business inkjet products.

Other Programme highlights include:
- A lease package for hardware and service with easy manageable payments.
- Supplies are charged on a per-page basis.
- The option to include a document managed solution to your programme: b-guard, offered exclusively through Brother
- Automatic meter reads to ensure complete accuracy with no administration.
- The “No Minimum” policy to ensure you only pay for the pages you print.
- Access to an online web portal to order supplies, log a service request, view device usage and individual running costs of each machine to ensure the right device is in the right place to run your business effectively.

For more information about Brother and its MPS programme visit www.brother.eu

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 first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

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

© Quocirca 2012 - 8 -