Achieving a Secure Print Infrastructure

Achieving secure printing for confidential documents is an ongoing consideration for all responsible and compliant IT departments. This white paper seeks to address the challenges and considerations, ramifications and benefits of achieving a sustainable, solid, demonstrable print infrastructure, otherwise termed as achieving a state of secure print.

July 2014
The Challenges

Most IT departments reluctantly consider print as part of their remit. Print has never been considered as either racy or viewed as innovative. It’s cumbersome, labor intensive and driven largely by the user, who has neither the inclination nor the responsibility to ensure print security, even when the documents carry the ‘confidential’ tag. The scenarios that typically lead to breaches form part of our everyday working lives, but they are worth examining-

Unintentional Breach Scenarios
An authorized internal user prints a confidential document to a shared printer. The user rushes to collect it, aware of its sensitivity. But, by the time he reaches the printer, it has been scooped up by mistake as part of a previous print output.

Or, frequently, with a myriad of printing devices available on their network, users send jobs to a different printer before resending to a closer machine, so now multiple copies sit unattended on the out tray of multiple printers in various locations.

Sometimes security breaches are caused by the increased functionality of the printer hardware itself. With today’s auto-standby green printers, dormant printers render themselves offline, leading users to print a further copy in frustration and several instances of confidential documents start to pile up.

Intentional Breach Scenarios
Disgruntled employees can take advantage of unintentional print errors. Intentional breaches are much harder to legislate for and their consequences are likely to be far reaching. Most firms will take extra precautions around HR and Payroll/Finance assigned printers, but are largely unable to secure the print facility for every member of management and their administrative support team who are also party to confidential information. Disgruntled employees that come into contact with unsecure confidential documents have an immediate weapon in which to progress their case against an organization. Various Data Protection and Freedom of Information acts across the globe mean that individuals have the right to see all data held against them and nothing acts quite like a starting point for a case as piece of indiscriminate print.

(Tip – Think it won’t happen to you? Quocirca Research** shows that 70% of organizations have experienced one or more accidental data breach through printing.)

Options in Achieving Practical Accountability and a Secure Print Framework

Once you have understood how real the print security threats are within your organization and how they could and do manifest, it is time to go back to the planning stage. Very few IT departments have ever had the luxury, in budget or time, to set out an Optimal Print Infrastructure; printers just tended to proliferate around us. Accurate and ongoing printer mapping used to be a recommended methodology for large companies, but in most enterprises that in itself has become too complex to sustain.
To set out a secure print framework, you should broadly consider three sequential steps:

- **Decide** – What level of print security you realistically need to achieve and how it can be best achieved.
- **Document** – Never forget that it is IT’s responsibility (not the named department on the printer) to achieve and demonstrate ongoing regulatory compliance when it comes to securing confidential print. Documenting results remains key - from cost savings to regulatory proof points.
- **Deliver** – A managed, automated, hassle and worry free print service.

We will briefly consider each of these areas in turn:

**Decide** – Clearly not all print is created equal and therefore it should be treated accordingly. Prioritize the departments where confidential documents proliferate and are vulnerable to breaches. Additionally, identify likely areas of continued misuse for personal print (More than likely, you will already know which printers consume extraordinary resources. Don’t be afraid to dig deeper on usage). Both sets of users then become your number one education targets, who need to understand the financial impact of breaches upon a company. (Tip – Empower and educate users with facts and figures on cost containment.)

**Document** – Document your findings and analyses, and recommend the appropriate course of action. In a litigation scenario, you will need to prove that your organization has adopted best business practice in order to protect confidential information. Consider also how external influences can alter the mix. Understand how you will incorporate evolving technology and user trends, such as personal and mobile devices due to the BYOD trends, and what your organization’s stance is towards printing out Website content - especially social media sites where the user has a freehand in content input. Provide proof that users are assigned printers via IP address, host name or user group membership to allow correct printer mapping to be apportioned at each location.

Wherever possible, try and simplify your print associated overhead. (Tip - If you are working in a VDI environment, check out the system stability benefits that Universal Printer Drivers can deliver, which seamlessly replaces all native Windows drivers in your infrastructure significantly simplifying printer management.) For cost justification, empower yourself with a detailed knowledge of your print overhead. Knowing how much it is costing you, (per person, per department, per location) is a powerful tool. Document and manage this ROI cost comparison at the start of the process and at six monthly review intervals. Only then will you fully understand the true cost of print (Staggeringly, Gartner estimates that print as a whole costs the average organization between 1 and 3% of total revenue*) and be able to accurately cross charge the actual costs of print to users and departments. You can also justify debates about internal print charges by demonstrating likely cost savings that can be enabled by easily automating standard print out policies – such as fast printing in black and white and duplexing. (Tip - Pull printing is widely noted to reduce paper volume by 20%; duplexing by default saves 30%.)

Without documented evidence, you have no tool for remediation. Therefore the selection of an archiving tool that allows print data to be archived in a database should be high on your deployment list for security and regulatory compliance. This also allows you a concrete, traceable reference point, if ever required, of who is printing what, where and when.

**Deliver** – Proof: don’t leave it to chance. Whilst education of users is essential, never forget that ultimately it is not their responsibility to provide secure printing. It’s yours. Secure pull printing, or sometimes referred to as ‘follow me’ printing, is a ‘must have’ in today’s litigious world, allowing users to release documents on any network printer in proximity after authenticating themselves.
Empower Sustainable Cost Reduction

In deployment, look for solutions that take the burden of delivery away from you, and that cover all IT platforms and integrate all printers on your existing fleet, regardless of make and model. Look for those solutions that offer sustainable cost reductions. It is worth noting that secure pull printing provides significant knock-on effects in carbon, electricity consumption and resource reductions. This consolidation, or virtualization, has successfully occurred right through data centers worldwide.

The era of printing virtualization is upon us with print appliances and print stream compression now taking the low powered load, high availability providing full redundancy, and centralized print servers dramatically simplifying print management tasks and driving down support costs. (Tip - Help desks typically log 50% of their calls as being printing related. With the enablement of printing virtualization, typically they receive an immediate 30% reduction in printing related calls.)

Conclusion

Essentially throughout the delivery process remember, the results will be worth it. Quocirca Research** showed up to 40% of savings on print costs for those that have deployed secure print.

Sources:

*Gartner Group, March 2009 Study
**Quocirca Research, January 2012

For more Information or a free product trial, please visit www.uniprint.net or e-mail marketing@uniprint.net.