STAPLES
Business Advantage®

Using Managed Print Services to Improve Document Security

A Staples, Inc. White Paper

Tech Solutions

Using Managed Print Services to Improve Document Security
By Staples® Business Advantage

Summary

Keeping data safe is a growing concern for companies of all sizes. Technology allows us to create documents on a wide variety of devices, store them on hard drives, network servers or in the cloud, and print them from a desktop or handheld device from anywhere in the world. Despite the fact that we live in a digital age, the promise of the "paperless office" has never materialized. In fact, the estimated number of office pages printed, copied and faxed annually in the U.S. peaked in 2007 at more than 1 trillion pages.[1]

With so much printing going on, enterprises are struggling to manage their printing environments to ensure efficiency, security and control. This problem has created one of the fastest-growing trends in printing today: Managed Print Services (MPS), which is expected to grow 20 percent each year through 2015, resulting in a market opportunity of about $78 billion.[2] Businesses are drawn to the projected 15 to 30 percent cost savings and attractive business benefits such as reduced downtime, increased staff productivity and reduced waste (paper, ink/toner, energy).

However, while MPS is a viable solution across many industries, Information Technology (IT) executives who work for healthcare organizations, financial institutions, government agencies and law firms, in particular are concerned about the access an MPS service provider might have to sensitive data. This is because MPS software taps into the network infrastructure, during the assessment process and ongoing monitoring, to report on device usage, repair issues, and ink and toner levels, and then automatically deploys the necessary "fix." However, these concerns are unfounded. MPS software has no access to the content being printed, faxed or scanned — only to the attributes of the print job itself. In fact, MPS helps to protect and control printed assets and can play a big role in ensuring sensitive documents don't end up in the wrong hands.

What are the benefits (and concerns) of MPS?

MPS is a service that helps IT departments reduce the total cost of ownership (TCO) for printers and related devices throughout the organization. Optimizing the printing infrastructure and implementing best practices not only reduces cost, but also helps to improve workflow and increase productivity. As good as this sounds, handing the keys to the candy store over to an MPS service provider should not come without due diligence. One of the most common questions asked by IT departments considering MPS is, "How can you guarantee that documents and confidential information on our network will remain secure?"

Maintaining a secure network is not just a business policy; it's the law. Healthcare organizations, for example, must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which enforces operating rules to ensure patient information remains confidential. A key tenet of HIPAA is that organizations will store personal medical records in a secure environment.

STAPLES Business Advantage®

[1] **According to InfoTrends, a Massachusetts-based market research and consulting firm.**

[2] **Photizo Group, 2011 MPS Market Size, Share and Forecast Study.**

Financial services organizations (banks, accounting firms, real estate appraisers, loan brokers, mortgage lenders and even debt collectors) must abide by the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999. GLBA compliance is mandatory and requires having a policy in place to protect nonpublic financial information from any foreseeable threats to network security and data integrity. There are myriad regulations across industries that are designed to protect personal information. Obviously, engaging an MPS provider must be done in a way that does not cause any regulatory violations.

Confidential healthcare, government, financial and legal information crosses through printers, scanners, copiers and fax machines all the time, primarily because signed and sometimes notarized hard copies of such documents remain the normal form of document exchange. These documents can include information like medical records, prescriptions, legal content and financial statements, so it can be challenging to comply with the law without stringent rules in place for tracking where these types of documents go and who can see them. An MPS provider can actually be a valuable asset in document management and security by deploying the appropriate devices and management software in the network, and implementing best practices in document management to ensure compliance with security policies and regulations.

What MPS can and cannot access on the network

The core components of MPS include an initial assessment, which provides a snapshot of the current printing environment, and ongoing monitoring of devices. Both of these functions are achieved using fleet management software that taps into the network for data analysis and tracking related solely to printing devices. The software is used to flag areas like over- and underutilized equipment, and device to end user ratio.

While skepticism about any outside entity — such as an MPS provider — connecting to the corporate network is inherent among IT executives, it should be understood that MPS software can only access device attributes — not systems, files or data. In fact, the MPS software can only access the same information you would see on a device operator panel. The only difference is that the software can accrue the information from every device on the network for analysis. This includes things like serial number, manufacturer model, map address and usage/page counts. The software can also detect file type (Word®, Adobe®, PowerPoint®, Excel®, etc.) and whether a document is being printed in color or black and white. This is mainly to help understand printing needs and the behavior of those doing the printing. But for security purposes, it is important to understand that, as documents are sent to a device, the software cannot capture an image or any content from the document itself.

These device attributes are used to optimize the print fleet — in most cases, this means removing unneeded devices from the fleet. Some companies can reduce their fleet by as much as 50 percent while still maintaining the printing needs of employees. Further analysis will also reveal opportunities to upgrade equipment or reconfigure the placement of existing devices. These optimization activities create a more efficient and cost-effective printing environment.

MPS software alerts the provider when there are service or maintenance issues, including which machine or part of the network requires repair. The MPS solution knows when ink and toner are running low and automatically orders supplies to be delivered when needed. It can also be used to improve printing behavior through rules-based document management at the desktop that suggests (or enforces) black and white vs. color, double-sided or draft-mode printing, and other approaches for reducing waste. Rules can also be added to route documents to designated secure printers.

As documents travel through the network to printing devices, how can IT executives feel confident the MPS software will not compromise document security?

Consider this analogy. Look at MPS software as a locked truck filled with confidential cargo that is being transported from Point A to Point B. The driver of the truck is concerned about:

- Getting the cargo to its destination as instructed
- Taking the best route to avoid traffic and detours
- Delivering the cargo to the right recipient
- Reaching the destination on time

The driver of the truck has no access to the locked container or knowledge of its contents, only access to the operations of the truck, like speed, fuel level, and air pressure in the tires, and factors like road conditions, weather, traffic, detours and time of departure. In addition, the condition of the truck and the route are automatically monitored by the dispatcher who can arrange for fuel, new tires and maintenance as needed.

Document security — technical and human

MPS software cannot compromise document security, but sending documents from a computer to another device can be a highly insecure process. Primary responsibility for document security lies with the company and its employees. Documents, even the most sensitive ones, can easily be sent to the wrong printer or accidentally left behind for an unauthorized person to pick up. Many confidential documents wind up in trash cans or recycle bins where they can easily be viewed by unauthorized personnel. There are steps, however, that organizations can put in place to reduce the risk of human error.

The first step is to work with an MPS provider that offers a vendor-neutral solution. This will allow the company to select the printing device and security features that best suit their needs, regardless of manufacturer.

As for hardware; printers, copiers, fax machines, scanners and multifunction devices today offer security features that can help eliminate mistakes. Some devices require a password or personal identification number (PIN) at the device before a document will print. Other machines accept a swipe or scan card or require a biometric fingerprint swipe for authentication.

Mobile printing software allows documents to be encrypted so they can securely traverse a cloud network to an independent mobile print location. A retrieval code must be entered at the device in order for the document to print — a valuable feature for maintaining confidentiality. This is especially relevant when printing outside of the corporate network. Mobile employees who print to the office can configure their print jobs to be sent to a secure server at the office where they can be retrieved later at the printer with a PIN.

There are other checks and balances IT departments can implement. For added security, device memory can be cleaned, purged or destroyed, either in house or using an outside resource. Vendors who specialize in this service are bonded and provide certification to verify that destroyed data is irretrievable. Each printing device should also be paired with a shredder, rather than a trash can or recycle bin, to immediately destroy documents printed by mistake or that are no longer needed.

If concerns remain about MPS software tied to the network, the IT department can deploy a network sniffer to monitor for spikes that would provide notification when large amounts of data were being retrieved.

End user education

The most effective way to ensure document security is to take control of the printing environment. MPS software offers insight into printing devices as well as careless printing behavior that can lead to a breach in security and costly violation of regulations such as HIPAA and GLBA. A good MPS provider will look at the complete printing workflow and identify red flags, then assign responsibility for document management from desktop to printer. The greatest protection against printer-related security violations is to effectively train all employees about company policies and procedures. The MPS provider can work with the company to determine best practices for training, and incorporate rules into the MPS system with desktop screens that direct print jobs to secure printers.

Conclusion

As technology continues to proliferate, so will security concerns. Digital documents are easy to copy, save, send and print, so it is critical to engender a work culture of heightened awareness of document security, while also implementing processes to reduce risk to a minimum. MPS is an excellent solution for reducing document security risk while significantly improving printer fleet efficiency. MPS also delivers operational benefits by offloading routine maintenance of the printer fleet from IT or office staff, while simultaneously improving workflow. A reputable MPS provider is also a trusted partner who can provide expert advice on hardware selection and the implementation of security measures at the device level.

While human beings will always be the biggest source of vulnerability for document security, partnering with an MPS provider can dramatically reduce the “human risk” by rules-based document management at the desktop. Ultimately, MPS can be the front line of defense in document security compliance.