The Quick-Start Guide to Print Security

How to maximize your print environment and minimize security threats
The Hidden Security Threat

What’s the first thing that comes to mind when you hear the words ‘IT security’?

If you’re like most people, you’ll probably think of malware, email scams and passwords that are easy to crack. Or maybe the high-profile cases of hacking we’ve seen in recent years, involving millions of users’ credit-card numbers and personal details.

But there’s another aspect that often flies under the radar: print security.

These days, multifunction printers (MFPs) are more like powerful computers. They’re connected to your network and the cloud, accessed wirelessly by mobile devices, and capable of scanning, routing, storing and sharing documents.

But the flipside of all that power and flexibility is a big increase in security risks if the printer isn’t securely configured.

This quick-start guide will highlight some of the most important issues, and give you the inside track on how to ensure your print environment is smart and secure.

Let’s dive right in.
The Top 3 Threats

UNCOLLECTED DOCUMENTS
It’s estimated that 25% of print jobs are never picked up by the users who printed them.¹ That’s a big waste both of resources (paper and toner) and effort (somebody has to remove the documents and get rid of them).

But even more importantly, it’s a significant security threat.

That uncollected print job could be sensitive commercial information such as your marketing plan, latest sales figures or a presentation to a client. Or confidential information, such as somebody’s performance review, bonus letter or personal details.

¹. Nuance – Based on Nuance Customer data / Internal Study of Help Desk Calls
The Top 3 Threats

UNSECURED DATA

Even if every print job is collected, you’re still not out of the woods.

If proper security isn’t in place, documents with sensitive and confidential data moving around your network – via a cable or wirelessly – can still be intercepted. And don’t forget that Multifunction printers (MFPs) nowadays also have hard drives to cope with complex print jobs. If data on the drive isn’t deleted after printing, it could be open to abuse.

70% of organizations have had a data breach in their print environment,² and 60% of all breaches are carried out within a matter of minutes.³ So tightening up print data security isn’t an optional extra – it’s an absolute must.

---

². 2010 “Annual Study: US Cost of a Data Breach.” The Ponemon Institute, LLC, March 2011
³. Verizon 2015 data breach investigations report
The Top 3 Threats

Mobile devices now outnumber people across the world, and are expected to grow exponentially⁴ to 11.6 billion by 2021. Bring your own device (BYOD) is becoming the norm, as people connect smartphones, tablets and laptops to the company network.

If organizations don’t provide a simple, cross-platform printing solution for these users, they may decide that a third-party app is what they need. And that’s a big threat, because unauthorized apps could seriously compromise network security.

The U.S. Department of Health and Human Services fined two hospitals a total of $5.3 million for improper management of paper records.⁵

---

⁴ Cisco Visual Networking Index
It’s Time to Take Control

The consequences of a printing security breach are too serious to ignore, and prevention is always better than cure.

A structured, multi-pronged approach will ensure that your print environment is protected to the highest possible levels. You’re going to need a mix of at least five capabilities.
It’s Time to Take Control

Secure printing means that confidential documents never lie unattended in paper trays. Print jobs are sent securely to the printer, and released only when the user enters a passcode or swipes an ID card.

Image overwrite is used by advanced printers or MFPs to electronically ‘shred’ documents that are held on the hard drive as part of print processing. This shredding can be carried out automatically, manually or on a schedule.

Data encryption keeps prying eyes from seeing sensitive information as it moves to and from your printer.

Network security prevents unauthorized remote access to your printer and protects confidential data as it moves across the network.

User authorization allows you to grant or deny access to specific MFP functions such as scanning or access to customer data. If you’ve already got access controls in place for other tech, this is how you integrate your MFPs into those policies.

Only 56% of SMBs include multifunction printers (MFPs) in their security strategy.6

6. 2016 Survey carried out by Coleman Parkes for Xerox
Don’t be a Soft Target

Organizations today realize the importance of having the latest version of software in the fight against security threats.

But it’s crucial not to overlook printer software when designing your print security strategy.

Next-generation multifunction printers (MFPs) are equipped with embedded antivirus software, so you’re safe against malware and other potential threats. They also have automatic firmware update functionality, so no user intervention is required.

GET TO KNOW YOUR USERS

It’s easy to think that all security threats are malicious and come from outside the organization. But in fact 35% of data breaches are internal, and simply the result of human error.\(^7\)

User analytics will let you see who’s accessing, sharing, scanning and printing documents. This user-centric view of your print environment will allow you to design policies and profiles to tighten your security – and control your costs.

\(^7\) 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute
Take Your Print Security to the Next Level

Print security is often neglected when organizations assess potential threats. But print data breaches have serious consequences – for customer confidence, your competitive position even and your bottom line.

Advanced print security solutions are available today to let you balance flexibility with security, control with ease of use.

They allow you to fully exploit the latest trends and technologies – such as mobile working and mobile printing – without compromising confidentiality or exposing you to unnecessary threats.

They harness the incredible power of MFPs, using next-generation technology to help you to stay smart and secure.

To find out more about print security solutions, talk to a Managed Print Services (MPS) partner today.
About Xerox

Xerox is an $11 billion technology leader that innovates the way the world communicates, connects and works. Our expertise is more important than ever as customers of all sizes look to improve productivity, maximize profitability and increase satisfaction. We do this for small and mid-size businesses, large enterprises, governments, graphic communications providers, and for our partners who serve them.

We understand what’s at the heart of work – and all of the forms it can take. We embrace the increasingly complex world of paper and digital. Office and mobile. Personal and social. Every day across the globe – in more than 160 countries – our technology, software and people successfully navigate those intersections. We automate, personalize, package, analyze and secure information to keep our customers moving at an accelerated pace.

For more information visit www.xerox.com.