Strategies to Secure your Print Environment

By Joe Zubeck

Security threats are constantly evolving, are ever-present, and are smarter than ever. Although it may not be top of mind when considering data security, a law firm’s print environment can be particularly vulnerable to threats. As the official print solution partner of KCMB and experts in print security, we recommend four steps to our clients.

1. Establish acceptable use policies for printers and document management.
   Our law firm clients often tell us stories of going to their shared multi-function printers to pick up a document, only to find scattered pages that had been printed and not picked up by another user. Look at the workflow of each user in your firm to determine the appropriate times for using desktop printers instead of shared devices, and the methods by which shared and desktop printers should be managed.

2. Require passwords for secure device management.
   Simply put, password control who has access to printers in your firm, and not only restrict the printing of documents waiting in a queue, but also the access to printer hardware and related devices. Today’s MFPs are complex embedded systems that contain full-scale operating systems, web servers, hardware and software interfaces, and more. They can streamline and simplify work, but also can potentially represent a serious risk to your network and enterprise systems if they are not adequately protected.

3. Implement document and device activity controls.
   A simple step for securing documents on shared devices is to require employees to login at the printer in order to print their documents, also known as pull printing, ensuring that sensitive documents are never left unattended.

4. Engage experts to create and maintain security measures.
   Security breaches happen when there are gaps in your security strategy, and when you rely on manual device configuration, it’s easy for those gaps to multiply.

imageQuest is a wholly-owned subsidiary of Xerox Business Solutions, Inc., which means we provide best-in-the-industry device and data security to our customers. Our Intelligent Workplace Services provide a powerful approach to MFP security with the ability to defuse threats at their source the second they occur, to keep you safe across security standards and policy management. Xerox ConnectKey devices are built to be trusted endpoints, to leverage innovative technologies to safeguard your critical documents and data. imageQuest provides:

Next-level security, right out of the box
- Built-in intrusion-prevention measures stop malicious attacks, malware proliferation, unauthorized device access and device misuse, whether from transmitted data or direct interaction at the device.
- Device detection sends alerts when a harmful change to the printer has been detected and ensures only authorized printers can access your network.
- Document and data protection blocks intentional and unintentional transmission of data to unauthorized parties with high-level encryption and safeguards for printing and scanning.
- Partnerships with security experts like McAfee and Cisco help you achieve the highest security standards and support compliance and certifications.

Instant, effortless, fleet-wide policy enforcement
- Easily create security policies that align with your precise IT requirements.
- Push new configuration device monitoring and regular, real-time compliance reporting.
- Rapidly identify and remediate non-compliance on one device or across the entire fleet.
- Receive ongoing performance reports that highlight areas for improvement and allow for easy adjustment.

Unmatched access control
- On-device authentication via ID card or PIN code means only authorized users can access fleet printers and specific print jobs.
- Pull printing ensures sensitive documents are never left unattended.
- Job tracking provides a complete audit trail of all device activity, highlights output behavior that may require investigation, and isolates print jobs that should be avoided.
- Chargeback and accounting tie all activity back to specific departments or projects to easily monitor costs.

Regulate restricted content automatically
- Administrator-chosen keywords and phrases trigger an immediate alert when any unapproved scanning, copying, or printing is detected.
- All documents managed by Intelligent Workplace Services are automatically encrypted using a symmetric key cryptography algorithm before being sent to content storage.
- Sensitive data is also secured through user- and group-based access, password protection, and automated retention and disposition.
- Governance and lifecycle management protect and retain important business information and provide visibility into who interacts with content and how.

Please contact Joe Zubeck at 913-693-8347 to schedule a print device security review and to learn more how imageQuest can help you achieve better data security for your firm and your clients.

ABOUT THE AUTHOR:

Joe Zubeck is a major accounts executive with imageQuest, and he has been with the company for 15 years. He’s also known to play a mean round of golf, and won the BBBC Longest Drive Contest in 2016 and 2017.