SMART CHANGE STARTS HERE.

BETTER AWARENESS FOR INCREASED VIGILANCE:

4 STEPS TO IMPROVING YOUR MULTI-FUNCTION PRINTER SECURITY

IDC Analyze the Future

Canon
CANON SOLUTIONS AMERICA

MINING THE BENEFITS OF EXPERIENCE

One advantage that has come out of the numerous data and security breaches over the past couple of years is an increased level of vigilance and interest in security on the part of the end user. Whereas in the past, providers often had to enforce the importance of security on customers, recently the customer has become more proactive in regards to security solutions.

This increased vigilance has expanded into a number of arenas that previously were not high-awareness areas. The multifunction printer (MFP), for example, has always been an area in which security can be compromised, based simply on the fact that one of the most common security breaches is confidential information left sitting in the output tray.

But today's MFPs are more than simply output devices—they are sophisticated network components with embedded web servers and the ability to connect directly to host applications and cloud-based services. Along with the obvious physical risks, the unsecured networked MFP can become vulnerable to malicious hacks and data breaches from outside the firewall. With that in mind, there are numerous problems that can present themselves when it comes to printer and MFP data security, and many solutions that can be employed.

END USERS ARE TAKING NEW INITIATIVES TO PROACTIVELY ADDRESS SECURITY SOLUTIONS.

THERE ARE MULTIPLE WAYS TO GRANT OR BAR ACCESS TO USERS.

STEP 1:

MANAGE ACCESS

Increasingly, IT administrators are tasked with managing user access to printers and MFPs. User authentication features such as passwords, cards, or biometric authentication can be used in follow-me or pull printing, ensuring that a print job is not output to a workgroup device until the user is at the device. These measures can also help reduce the risk that documents could be e-mailed or faxed without authentication, helping to prevent secure documents from being inappropriately distributed, or allowing for an audit trail if they are. Additionally, different levels of access can be granted to various users, blocking guests or low-level employees from more sensitive material, higher-level functions, and server-level access.

STEP 2:

ADDRESS CONCERNS WITH SECURE MOBILE PRINTING

Continued use of mobile technologies in the corporate sector is creating a whole new set of security risks and potential vulnerabilities. While its adaptation has not necessarily been as quick as some might like, there is no question that the ability to print from tablets and smartphones is in demand. A 2015 study by International Data Corporation (IDC) found 75 percent of users said the business value of mobile printing was similar to PC printing, and 15 percent said it was greater.[1]

As mobile printing becomes more common, a core question exists in regards to who is allowed to print and on which devices. As with the authentication measures mentioned above, mobile device users can be granted varying levels of access to workgroup MFPs, ensuring that secure data is controlled, and that all data is limited from entering or leaving the network without proper authorization.

A 2015 IDC STUDY ASKED RESPONDENTS TO QUALIFY THE BUSINESS VALUE OF MOBILE PRINTING IN RELATION TO PC PRINTING.

75%
SAID "SIMILAR"

15%
SAID "GREATER"

1. IDC, Mobile Device Users/Non-Users: Print, Scan, Document Management, Worldwide

STEP 3:

SECURE HARD DRIVES

The internal storage device of an unsecured network printer can be a threat to security, not just while the device is in active use, but afterwards. User authentication can help control access to the documents and data stored on the drive, as they can be encrypted to allow only certain users access. Disk encryption features can also protect data in the event of the physical theft of the device or drive—the Advanced Encryption Standard (AES) is recognized as a preferred form of encryption, so it is advisable to ensure an MFP meets this standard. An additional layer of security can be found in a Trusted Platform Module (TPM), a dedicated microprocessor that can secure hardware through cryptographic keys. The sensitive data is stored separately from the MFP and ensures the MFP's hard drive will work only on the device containing the original TPM.

Automatic disk wiping and log wiping are also important features not-only to have, but to enable. And when an MFP reaches end of life, before disposal the hard drive should be wiped to a level that meets what are often strict levels of compliance required by various industries.

MFP INTERNAL STORAGE DEVICES PRESENT ANOTHER LEVEL OF RISK.

STEP 4:

SECURE THE NETWORK

The Internet of Things (IoT) practically began with the networked printer, and by definition, the data traveling to and from an MFP is vulnerable to hacking, viruses, and other breaches. While there is frequently a perception that IT departments don't work on printers, the truth is that printers are an integral part of the network that are vulnerable and must be secured. MFPs should be behind a firewall, just like every other network-enabled device, and SSL encryption should be used for the web interface.

As with most devices on the network, user education and compliance is key to ensuring the security of the network. Awareness of the MFP as a fully integrated, networked device vulnerable to the same issues as a computer is key for all users, from the CIO on down.

DATA TRAVELLING TO AND FROM THE MFP IS VUNERABLE TO HACKING.

CANON SOLUTIONS AMERICA

CANON SEE IMPOSSIBLE