PaperCut

Centric Business Systems

Print Security Checklist

Use this checklist to assess the security health of your print system:

1. Securing Print Infrastructure

- [ ] Is there secure network communication between the end user and the MFD?
- [ ] Have you separated the print server from the network to protect traffic from interception?
- [ ] Are you monitoring and investigating any packet sniffing or port scanning behavior on the network?
- [ ] What happens to your print data during network outages?
- [ ] Are you hiding document names in your print queues?
- [ ] Have you disabled the USB ports on MFDs to prevent someone from scanning to USB devices?
- [ ] Has all unused MFD functionality been disabled?
- [ ] Have you applied all patch updates and do you have a security patch update procedure that tackles the latest vulnerabilities as they happen?
- [ ] Is there any sensitive network information stored in your MFDs? Are device passwords (such as the admin password) updated and secure?
- [ ] What happens to your devices at the end of their life? Does the hard drive and internal memory of every printer get erased and securely disposed of at the end of its life? Are you adhering to industry standards, such as specifications established by the US Department of Defense (DoD)?
- [ ] Has your organization invested in any Data Loss Prevention (DLP) technology? If yes, how is this complemented or compromised by your print security?
- [ ] Are the same print security settings employed consistently across all devices from desktop PCs, to tablets and smartphones?
- [ ] Are your MFDs secured or located in a position where CCTV cameras or people can view them so that malicious activity can be both detected and deterred?

2. Securing Print Workflows

- [ ] Can anyone (even a visitor) walk up to your MFDs and copy, scan, or fax any document?
- [ ] Can they scan any document to a folder, email, or fax?
- [ ] Are printed jobs left unattended in the output trays of printers and copiers?
- [ ] Can users bypass the system and print directly from a print server or a local queue on their computer to the IP address of a printer?
- [ ] How are you encouraging and enforcing your print policies?
- [ ] Are you enforcing a secure print release policy?
- [ ] Have you enabled print job timeout for older documents on your print server?

3. Securing Printed Output

- [ ] Do you maintain an audit trail of print, copy, scan, and fax activity? That is: who, what, when, where, and how?
- [ ] When archiving documents, are you using a file format that allows for long-term preservation?
- [ ] Do you use watermark technology to help classify sensitive documents and highlight what is vulnerable? Do you use digital signatures to identify who printed a document?
- [ ] Have all end users been adequately trained, not only in how to use a print system, but also on what your organization's print policies are, and the impacts of policy breaches to your organization?