Erb's Technology Solutions
Connecting People with Technology

CHECKLIST

EXPOSING PRINT VULNERABILITIES:
TRUST ETS AND HP TO KEEP YOUR DEVICES SECURE

Printing and imaging devices are prime sources of proprietary information, yet only 18% of companies monitor their printers for threats.[1] Do you?

Printers and other print devices are innocuous staples in any business environment — but they also have the power to bring your business down. Without the proper protocols and security in place, forgotten printouts or even unauthorized repair personnel can lead to a breach that puts your network data and resources at risk.

At Erb's Technology Solutions (ETS), an HP Gold Partner, we offer HP Print Security Solutions that can integrate smart hardware and software solutions with your larger IT security plan to protect the sensitive information in your printed documents.

Let ETS help you explore how HP printers are designed to work with security monitoring and management solutions to help reduce risk, improve compliance, and protect your network from end to end. We offer the knowledge and solutions to help you:

- Encrypt storage with secure erase
- Securely eliminate old data from hard drives
- Vet printer maintenance vendors
- Disable unused ports and protocols
- Control administrative access

Print security requires a combination of data, devices, management, and human resources — all of which you can get by partnering with ETS and HP. HP Print Security Solutions can help safeguard your business against threats while increasing your confidence and vigilance inside company walls.

Visit our website to learn more.

Here is a quick checklist of vulnerabilities that show the various ways your print devices can be misused, hacked, or otherwise neglected, leading to breaches that jeopardize your business data:

□ **Control Panel** — The settings and functions of your printer devices can be accessed by nefarious users looking to exploit the device and even disable it completely.

□ **Open USB Ports** — Unsecured USB points, network ports, and protocols like FTP and Telnet give unauthorized users access into your print devices' jobs, data, and settings.

□ **Input and Output Trays** — Does your company offer documents printed on special paper? Letterhead, prescription sheets, and even checks can be tampered with or stolen from unsecure input trays, while the output trays offer easy access to sensitive documents that have yet to be retrieved.

□ **Mobile Printing** — On-the-go professionals can accidentally print sensitive documents or forget to pick them up from output trays when they are back in the office, leaving data there for the taking.

□ **BIOS and Firmware** — Firmware that becomes compromised during startup or while running, can open up print devices, and the network at large, to attack.

□ **Network** — Just as networks can be hacked, so too can printing jobs. As the requests fly through your communications, print jobs can be intercepted and diverted to give criminals access to the data on them.

Erb's Technology Solutions
4935 Bowling St SW, Suite E | Cedar Rapids IA, 52404 | 800.369.3727 | www.etsconnect.com

[1] Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016.

hp Partner First Gold

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.