General Data

Smarter Technology. Exceptional Results.

Don't Become Another Security Breach Statistic

"In 2019, printers are 68% more likely to be the source of an external breach." - Spiceworks Survey

Imaging and Printing Vulnerability Points

Capture - MFPs can easily capture and route jobs to many destinations, potentially exposing sensitive data.

Storage Media - Imaging and printing devices store sensitive information on internal drives or hard disks, which can be accessed if not protected.

Cloud-Based Access - Unsecured cloud connectivity may expose data to unauthorized users.

Control Panel - Users can exploit imaging and printing device settings and functions from an unsecured control panel and even disable the device.

BIOS and Firmware - Firmware that becomes compromised during startup, or while running, could open a device and the network to attack.

Ports and Protocols - Unauthorized users can access the device via unsecured USB or network ports or via older protocols (such as FTP or Telnet).

Output Tray - The output tray is the most common place for sensitive documents to fall into the wrong hands.

Input Tray - Special media for printing checks, prescriptions and other sensitive documents can be tampered with or stolen from an unsecured tray.

Mobile Printing - Employees who print on the go may accidentally expose data, or leave printouts unsecured.

Management - Without adequate monitoring, security blind spots across your fleet may remain undetected and increase costly data risks.

Network - Printing and imaging jobs can be intercepted as they travel over the network to and from a device.

Contact General Data today for a complimentary print risk assessment.

www.general-data.com | talktous@general-data.com | 844-643-1129