Printer Security Plan Checklist

Printers and MFPs are often overlooked as entry points to a company's network and are easy targets for cyber criminals. Addressing the topics on this checklist in a printer security plan will help minimize cyber security threats through company printers and reduce the possibility of a successful attack.

☑ Take Inventory

Older machines may not accept updated software or patches and create vulnerabilities for the network and business systems. Updates and patches install necessary security features which are needed to protect your network and business systems from getting attacked.

☑ Conduct Printer Security Assessment

Evaluate your equipment and know what the vulnerabilities are with each machine. Printers that are connected to the internet create a higher risk for a data breach. Identify what access is available on each printer and who has access.

☑ Adopt Secure Follow-me Print

Printed pages are often left on the printer for an extended time or sometimes get picked up accidentally by someone else. This can result in a security breach if the printed pages contain sensitive information. Establishing a secured output that requires user authentication before printing eliminates abandoned prints.

☑ Monitor Print Environment & Activities

Monitoring tools allow companies to track users and unauthorized users across all print devices. Installing auditing tools allow visibility into logs that identify users, time of use, and details about print functions used.

☑ Encrypt/Wipe Stored Data

Encrypting stored data on printers ensures that data is secure and isn't accessible if there's an unauthorized breach. Periodically wipe or overwrite hard drives when printers are stored are no longer used.

☑ Create Printer Security Policy

A policy that includes many of these listed best practices will set the standards and expectations for the entire company on the use of printers and MFPs. It can outline privileges based on user roles and grant rights for specific features.

☑ Educate Users

Educating users about cyber threats, protecting sensitive data, and newly drafted printer security policies is a best practice that should be followed. Employees are often the first line of defense against cyber attacks. Train employees on how to use printers to minimize security risks.

☑ Partner with a Managed Print Services Provider

Companies with limited personnel and skill will often rely on managed print service providers to assist with evaluating, monitoring, or managing their printers and printer security.

VISUAL EDGE IT