Securing Your Print Environment with DBS Managed Print Services

Secure, Compliant and Cost Effective

USB & External Device Vulnerabilities

ISSUE & RISK

Issue: Open USB ports can introduce malware.

Risk: Malware spreads across the network; no visibility or control.

SOLUTION

- Restricts or disables USB access
- Centralized monitoring of external connections
- Enforces consistent security policies
- Modern printers self-heal upon threat detection

Unattended or Unclaimed Print Jobs

ISSUE & RISK

Issue: Sensitive documents left on trays risk exposure.

Risk: Data leaks, compliance breaches, internal exposure.

SOLUTION

- Follow-Me Print (authentication required)
- RFID, badge, or PIN access
- Auto-deletes unclaimed jobs
- User awareness programs promote responsible printing

Outdated or Unprotected Firmware

ISSUE & RISK

Issue: Old firmware exposes printers to cyberattacks.

Risk: Exploits, data theft, system-wide infiltration.

SOLUTION

- Automates firmware & security updates
- Proactive monitoring & alerts
- Retires unsupported/end-of-life devices

Unsecured Network Connections

ISSUE & RISK

Issue: Printers connected without encryption or segmentation.

Risk: Intercepted print jobs, weak-password access, backdoors.

SOLUTION

- Strong password policies & authentication
- Network segmentation for printers
- Continuous monitoring & auditing

Runtime Attacks & Unauthorized Access

ISSUE & RISK

Issue: Smart printers are vulnerable endpoints with OS, storage & web interfaces.

Risk: Unauthorized access, altered jobs, undetected incidents.

SOLUTION

- Real-time intrusion detection & monitoring
- Access controls & secure authentication
- Detailed audit trails for compliance
- Continuous oversight across print ecosystem

DBS Digital Business Systems
Your Print and Technology Partner