imageOne
Easy, Efficient, Reliable.

5-Point Printer Security Checklist

HP reports that there are hundreds of millions of printers in the world and less than 2% are secure. We've outlined 5 points you'll want to ensure you include in your security strategy:

1 **Printer Security Policies Implemented and Followed**

A lack of printer security policies can leave organizations vulnerable to a costly data breach. Here are a few examples of what you should include in your Printer Security Policies:

Conduct a security risk analysis before deploying printers.
   – Change the default password to the administration control panel webpage.
   – Use encrypted connections when accessing the printer admin control panel.
   – Don't run unnecessary services.
   – Update and patch.

2 **Update Firmware**

   – Most companies would never miss a security patch on their PC fleet, but many allow their printer fleets to fall behind. In fact, over 55% of the 1.2 million printers tested by HP were on security patches.
   – Firmware updates also make systems more efficient, leading to increased performance and speed.
   – Ensure your hardware isn't too aged to receive firmware updates.

3 **Implement Anti-Malware**

   – Most companies impose strict anti-malware software on all PCs, however, printers are equally vulnerable and are often left to operate without these protections.
   – Anti-malware can help stop malware attacks on a computer or system by scanning all incoming network data for malicious software and blocking any threats it finds; it may be able to detect and offer specific protection against advanced forms of malware.

4 **Ensure Proper Configuration**

Don't make the mistake of retaining default security settings on your printers, which can leave dozens of open ports and protocols for potential misuse and access to the network.
   – Nearly 60% of companies fail to apply their own user password policies on their printers.
   – More than half of today's businesses use generic admin accounts to manage their printers.
   – 86% of businesses do not encrypt sensitive print-data motion.

5 **Threat Monitoring / Log Management**

Most companies wouldn't know if one of their printers was compromised.
   – 85% of companies don't enable print logs to track login attempts and user access.

Schedule a complimentary consultation with imageOne to determine if a no-cost security assessment is your next best step.