Listicle

Why Bring Your Own Printer could be a recipe for trouble

3 risks of leaving hybrid workers to their own devices

To enable print for remote workers, many organizations naturally leaned towards the obvious option of allowing employees to use their home printer, otherwise known as Bring Your Own Printer, or BYOP. In a recent study by Quocirca, it was revealed that while 86% of remote workers have a printer at home, only 17% of them were provided a printer by their employer for work purposes[1]. However, BYOP introduces a number of hidden risks and issues—here are the top three:

1. BYOP can create security risks
2. BYOP may lead to compliance violations
3. BYOP can reduce productivity and satisfaction

Read on to learn more about these risks and the best solves to successfully deploy a work from home or hybrid work print environment.

1. BYOP can create security risks

Between the lack of built-in security and poor personal security habits such as not changing the default credentials, home-use printers are ill-prepared for cyber-attacks. In one study, researchers found that 56% of the internet-connected printers they tested were vulnerable to being taken over by attackers[2], while another group of researchers were able to steal documents such as pay stubs and building plans stored in the memory of consumer printers[2].

By connecting consumer printers to your network and allowing employees to print work documents on it, organizations expose themselves to the risk of attackers gaining root access to the printer and using it to:

- Send out fraudulent emails using legitimate accounts stored in the printer, and more[3]
- Remotely execute unauthorized code to deliver malware
- Re-route print jobs to steal data
- Modify documents, such as the address on shipping labels, as they are being printed
- Gain access to the rest of the network

2. BYOP may lead to compliance violations

Only
1 in 3
employers track printed documents with confidential information[1]

Working and printing from home may inevitably result in confidential information such as payroll, addresses or medical information being printed. With a BYOP setup where printer make, model and functionality can differ from employee to employee, gaining visibility over these prints will be a challenge. In fact, only 1 in 3 employers have been tracking these documents[1].

With no visibility into remote print jobs, organizations will not be able to ensure that printed documents containing sensitive information are handled and disposed of securely. More worryingly, printing confidential information means a copy of the data resides within the printer's memory—and consumer printers are not equipped to handle these in a compliant manner, putting the company at risk of breaching data privacy and security regulations such as HIPAA or the GDPR.

3. BYOP can reduce productivity and satisfaction

Productivity has been one of the unexpected benefits of working from home[1] – but BYOP can eat into some of that. Consumer printers are often lower-specced than enterprise printers, and the difference in performance has been noticed, with remote workers citing print speed as the top benefit they miss while working from home[1].

Additionally, BYOP printers are not part of the enterprise managed fleet, requiring remote workers to manage their printers themselves. This can lead to a significant increase in unexpected downtime when supplies run out or if the printer needs maintenance.

Finally, with a BYOP setup, remote workers will not have access to the on-printer productivity apps that may be a part of their regular workflow, disrupting their productivity and creating barriers for collaboration.

Solve hybrid printing with HP Managed Print Services

Instead of relying on employees' home printers, your organization can engage an expert such as HP Managed Print Services for help to:

- SEAMLESSLY DEPLOY AND MANAGE YOUR HYBRID PRINT FLEET
  under the same MPS contract by including your remote workers and branch offices with HP Flexworker Service.

- ENABLE EMPLOYEES TO SECURELY PRINT FROM ANYWHERE
  with HP Secure Print, which holds encrypted print jobs until the employee is ready to retrieve the prints from an approved printer.

- PROTECT SENSITIVE DATA AND YOUR REMOTE DEVICES
  with end-to-end data encryption, hardware-enforced device security, and fleet-wide security policy management and enforcement—all part of HP Wolf Security.

- DIGITIZE AND OPTIMIZE PAPER-BASED PROCESSES
  via HP Workpath, which provides a rich library of apps to simplify multi-step document workflows and provide a consistent print experience at home and in the office.

Hybrid working is now firmly entrenched. Your organization's need for distributed printing might grow against this backdrop, but it's best to steer clear of BYOP. With HP MPS, organizations can make hybrid printing an easy solve with secure hardware, enabled with flexible services, and cloud-powered workflow and management solutions to empower your connected workforce.

Contact an HP Managed Print Services Representative

hp.com/go/mps

References:

1. Quocirca, Home Printing Trends Study, Jan 2021
2. Infosec, Securing the home office: Printer security risks (and mitigations), Dec 2020
3. Booz Allen Hamilton, Printer Vulnerabilities Leave Companies at Risk, 2018