REMOVING THE HIDDEN SECURITY AND COMPLIANCE RISK ON YOUR NETWORK

With data being termed by many analysts as "The New Oil", security and governance is more important than it has ever been, especially when organisations are under increasing pressure to adhere to regulation and legislation. So why do so many overlook an area that leaves their network and their data vulnerable?

Not us we hear you say. However, when DTP have conducted the most basic security assessment for some businesses and presented back our findings, many have been staggered by what we have found. So, what is the technology hiding in plain view on your network?

WOULD IT SURPRISE YOU TO HEAR THAT IT IS YOUR NETWORK ATTACHED PRINTERS AND MFDS?

If we were to ask an organisation if they have a firewall protecting their security perimeter, they would probably say yes. If we were to ask if they have two factor authentication and anti-virus and malware protection on their client devices, the answer again would most likely be yes. And if we were to ask if these devices were kept up to date in terms of firmware revisions, the answer would again be yes.

SOLVING IT TOGETHER

Telephone: **0113 276 0210** | Email: **MPSteam@dtpgroup.co.uk** | Web: **www.dtpgroup.co.uk**

SOME ORGANISATIONS ARE NOT APPLYING THE SAME ESSENTIAL SECURITY BEST PRACTICES TO THEIR PRINTER AND MFD ESTATES.

After all, modern MFDs are essentially network PCs that print, copy and scan. They have hard disk drives, keyboards, LCD control panels and they are attached to your network. They also have firmware and software: printers and MFDs have built-in operating systems, run executables, have DLLs, and run common protocols.

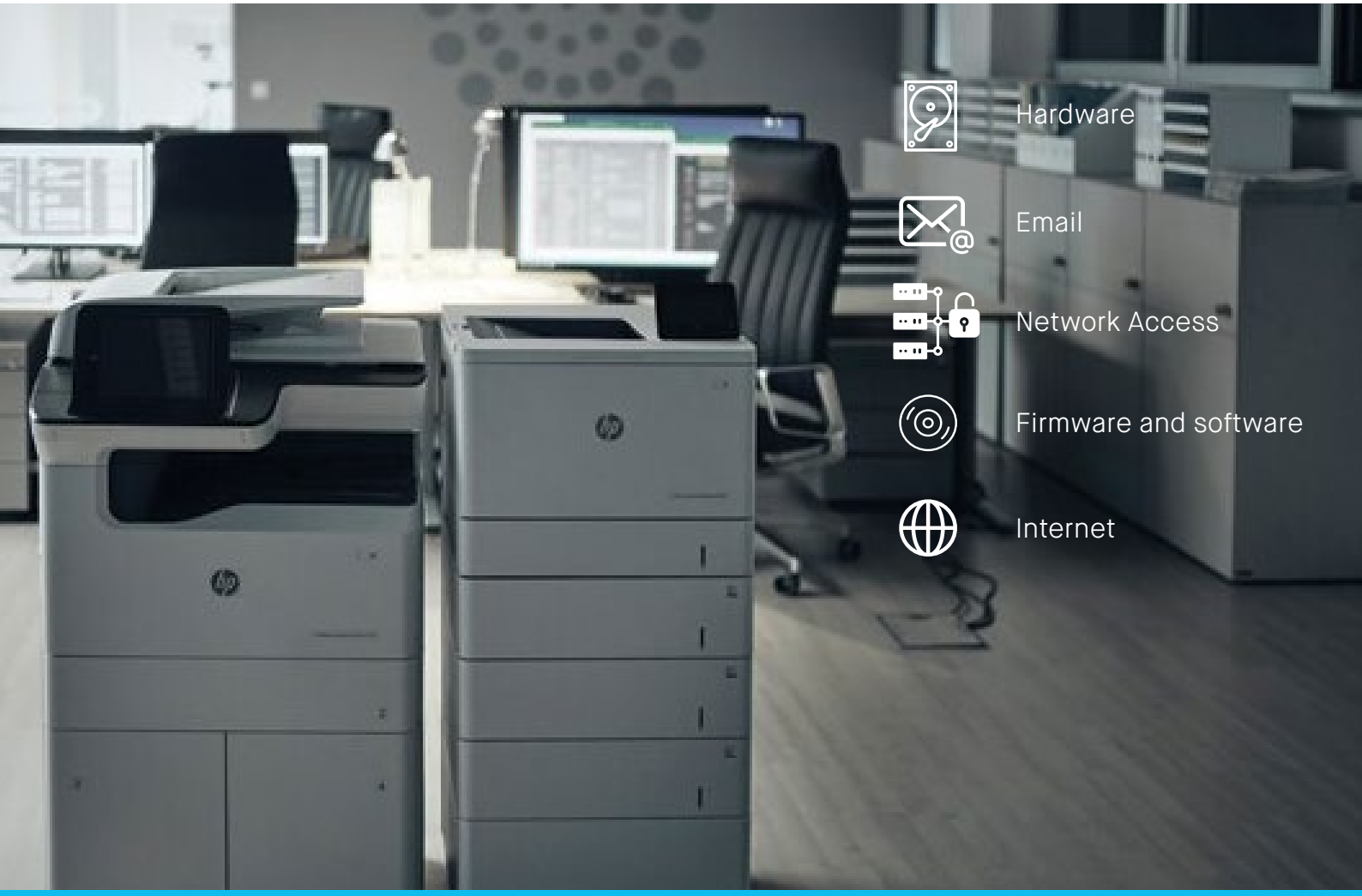
What's more, they are connected to the Internet and can be used to send emails. So with today's printers and MFDs being a fully functioning client device on the network, they require the same degree of protection, management, updates and monitoring as your PCs.

So, why are organisations continuing to overlook this potential hole in their security? We believe it is a combination of things:

- The device centric (as opposed to IT centric) nature of the Managed Print Service (photocopier) sector
- The pedigree of a number of leading vendors with that photocopier background
- The fact that in many cases, the MPS contract has typically sat outside of IT for decades

One thing we do know is that print related infrastructure is now being viewed by organisations as one of the top security risks, and this concern is growing according to a new print security report by Quocirca. 66% of organisations rank print in their top 5 security risks, second only to cloud-based services at 69%.

How then does an organisation take themselves from a position of risk and legislative non-compliance to one where their print environment is secure, pro-actively managed and monitored, and the legislative compliance and data governance tick boxes are not only ticked, but remain ticked?



AN INDUSTRY FIRST IN PROACTIVE PRINT SECURITY MANAGEMENT

We believe that the first step on any journey to best practice is understanding your current position. After all, if you do not identify the starting point of your journey and plan accordingly, the challenge of reaching your intended destination in the most efficient and cost effective manner becomes increasingly difficult.

In terms of supporting you on this journey, the starting point with DTP is a consultative assessment - whether that be a very simple questionnaire with a DTP Print Security Consultant as a low cost activity, or a more detailed one to three day piece of consulting - the outputs will give you detailed insights and recommendations to help you meet various compliance requirements (including GDPR).

THE RANGE OF CONSULTATIVE PACKAGES INCLUDES...

1. BASIC PRINT SECURITY ASSESSMENT INCLUDING SECURITY MANAGER QUICK ACCESS

This basic service includes a face to face meeting with a DTP Print Security Consultant who will work with you to answer a series of online questions and the responses will provide a basic overview of potential risk and recommendations. This service is vendor agnostic however if you are a HP user, then as part of this service we are also able to analyse a subset of your devices to determine their vulnerability. If they are not properly configured, devices can be a point of entry for a breach, allowing hackers access to the network. Settings such as Admin (EWS) Password, FTP, Telnet, Novell and USB Ports are often overlooked and it's critical to close the opening before hackers ever get in.

DTP performs this Quick Assess review on up to 50 of your devices against 15 essential security settings that we believe should be addressed on all printers and MFDs. At the end of the assessment, we provide you with a status report to view the risks imposed by missing, inconsistent and poor configurations and help you to determine what action needs to be taken to maintain compliance.

2. HP PRINT SECURITY BASELINE ASSESSMENT

This one day on-site security assessment is carried out by an experienced Print Security Consultant and provides a baseline indication of print security risk and compliance (up to 30 security controls). The output is a report with recommendation on how to reduce risk and improve compliance and includes a hands on demonstration on how to check covered controls. This service is tailored to smaller to medium organisations, typically where an organisation's IT team is responsible for security.

3. HP PRINT SECURITY ADVISORY SERVICE

This advanced three day on-site assessment is carried out by an experienced Print Security Consultant and provides an in-depth assessment of security risk and regulatory compliance (90+ security controls). As with option 2, the output is a detailed report with recommendations on how to reduce risk and improve compliance. This advanced option also includes details on each risk identified, together with detailed recommendations on mitigation (including a custom recommended roll-out timeline). This service is tailored to enterprise sized organisations and those within highly regulated industries with CISO or dedicated security teams.

After taking advantage of one of our print security consulting services, clients can then work with DTP Consultants to scope and implement one of a range of solutions and services tthat we offer. We take clients on a journey to best practice, as well as peace of mind from a risk and compliance perspective.

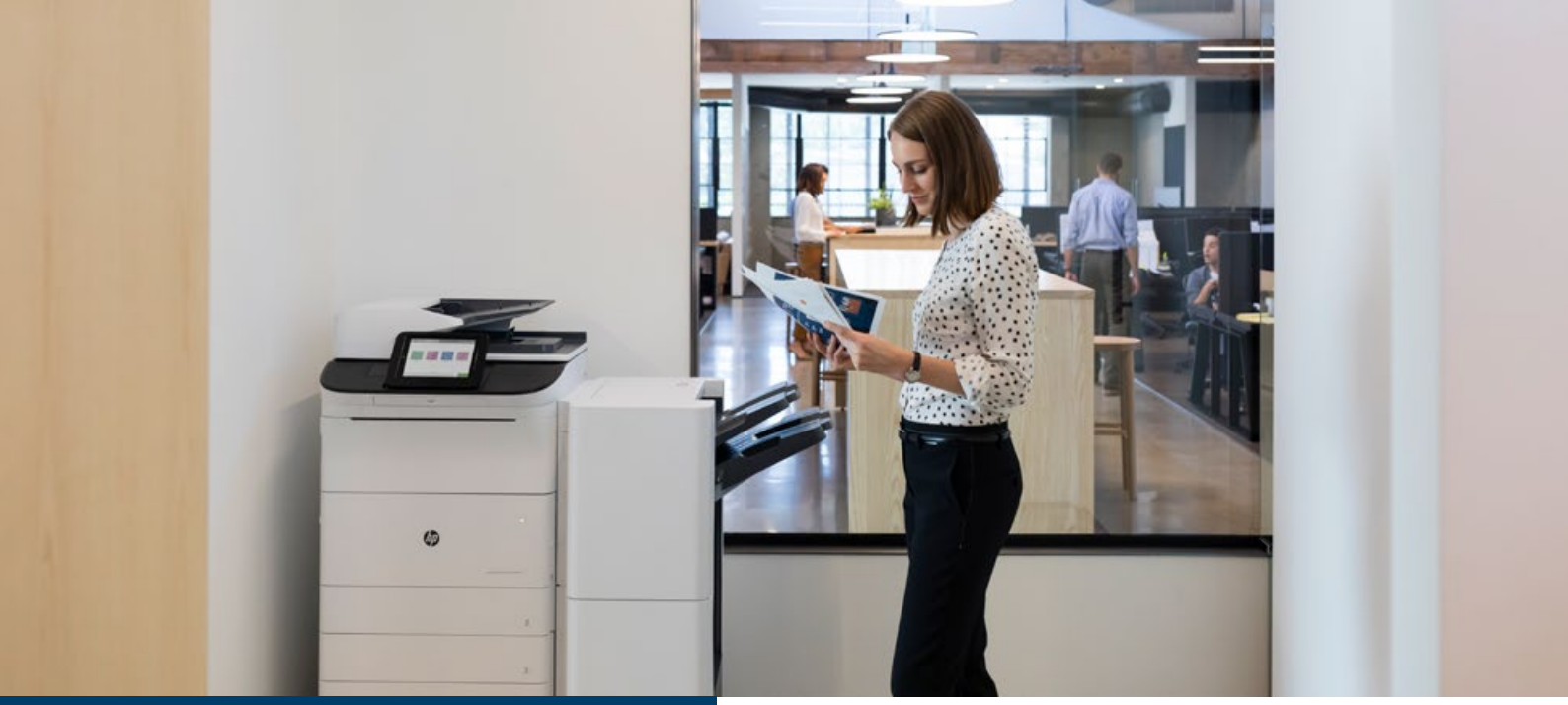
This could include the deployment of on-site print security policies, management and remediation software tools or the implementation of DTP's new DTP's Print Security as a Service (PrSaaS), offering – a new service providing you with all these options and much more within a simplified approach to fleet security on a pay per device, per month subscription service.

IN SUMMARY

DTP's print security practices can offer a range of services and solutions making it easy to monitor and protect your entire networked print fleet:

- Strengthen compliance to agreed corporate security policies
- Streamline security management by automating many processes
- Provide efficient fleet management of device firmware and certificates, ensuring both are kept up to date
- Secure new devices added to the network immediately

Telephone: **0113 276 0210** | Email: **MPSteam@dtpgroup.co.uk** | Web: **www.dtpgroup.co.uk**



WHY DTP'S PRINT SECURITY-AS-A-SERVICE?

As IT moves more and more to as-a-Service type offerings, you can fast track your compliance and risk governance around print security by adopting DTP's PrSaaS, the first service of it's kind to be launched on the market.

MINIMISE THE INVESTMENT NEEDED IN TIME AND MONEY.

DTP's PrSaaS helps you get to good quickly. After conducting their assessments, our Print Security Consultants will help you to devise a plan to mitigate your risk and work with you to tailor the print security policies to meet yours and your industry requirements. We will quickly implement the solution which is delivered as-a-Service and billed on a pay as you use basis, so there is no need for any capital outlay.

AUTOMATED POLICY ENFORCEMENT AND ESCALATION.

Once the solution and policies have been deployed, the policies are automatically policed. If a setting on a device changes, the solution alerts the DTP Print Security Monitoring Centre and automatically changes the setting back to the agreed policy. If there are repeated changes on a device, then our Print Security Monitoring Centre will escalate to on-site personnel who can attend the device and investigate.

REDUCE RISK WITH COMPREHENSIVE SECURITY FLEET REPORTING.

As part of the service, we provide detailed monthly reporting of the fleet covered, including details of any alerts during the month; their severity, escalations, along with our observations and any recommendations.

PROTECT YOUR DEVICES AND WORKFLOW WITH FLEET-WIDE FIRMWARE AND CERTIFICATE MANAGEMENT.

Keeping your printer and MFD firmware up to date is essential. We have lost count of the organisations we have worked with who we have found to be vulnerable from old firmware which can often be seven plus years old. As further threats are identified and new firmware is introduced, DTP is able to test within your print environment, then implement them to make sure any threats are negated.

Our team are experts in managing printer and MFD firmware. It's essential that new firmware is tested with your environment prior to roll out as in some cases, firmware can introduce issues with other software deployed on your devices. DTP ensure the latest safe firmware version is installed and we work alongside the respective vendor to develop patches to fix the issues.

Certificates are vital in protecting the flow of information to and from your devices. They are used to prove identity and encrypt data, enabling secure communication between trustworthy entities. Manually installing unique certificates can be an error-prone, laborious and time consuming task - up to 15 minutes per device in some cases. This causes many to opt-out of using certificates entirely or maintaining them properly. Our innovative technology solution streamlines this process by deploying unique identity certificates across your fleet with continuous monitoring to ensure validity and automatic replacements for revoked or expired certificates.

GET STARTED TODAY.

Printer and MFD Security can be daunting and we understand that it is a process, not a quick fix. So talk to DTP about how we can help you on your journey to compliance - get in touch for more information or to book an initial discussion with one of our Print Security Specialists.

0113 276 0210
www.dtpgroup.co.uk
MPSteam@dtpgroup.co.uk