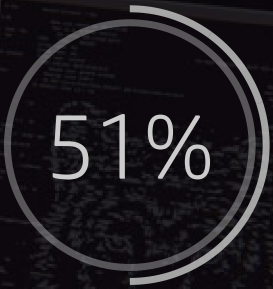
Top 5 security vulnerabilities of corporate print fleets

Cybersecurity risk is everywhere in your organization. But, did you know that some of your biggest vulnerabilities are hiding in plain sight? Fact is, if you are like the large corporations we've assessed, your organization isn't covering common cyber-hygiene practices with your MFP and copier fleet.

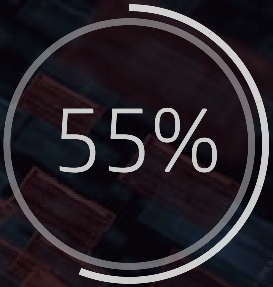
1.No policies in place

Only 51% businesses assessed had a formal print-security policy[1]



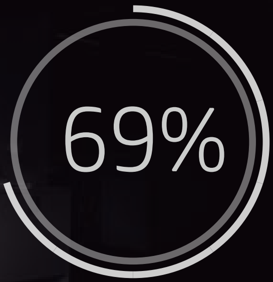
2.Lax on firmware

Over 55% of the 1.2 million printers tested by HP[2] were behind in security patches



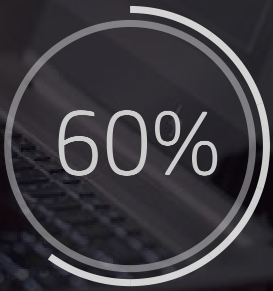
3. No anti-malware

69% of businesses don't have anti-malware on their printers[1]



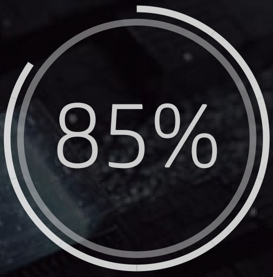
4.Wrong configurations

Nearly 60% of companies fail to apply the company's own user password policies on their printers[1]



5. No log management or threat monitoring

85% of companies don't enable print logs to track login attempts and user access[1]



Assess your risks to get ahead of them

How many of these risks apply to your organization? Contact us to learn how we can assess your security practices against common security and compliance controls.

The first step to protecting your data is uncovering your risks. Contact us to learn more.

[1] Common findings of risk assessments: Stats are calculated by HP using an internal database of results from assessments of 78 Corporate Enterprise organizations. Assessments conducted by the HP Print Security Advisory team from July 2015 to February 2019.

[2] 55% of printers behind in security patches: Based on data from 1.2 million printers, using the HP firmware security tool with 6505 Enterprises as of 3/28/2019.