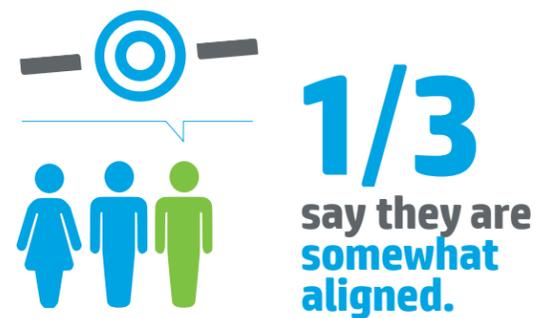
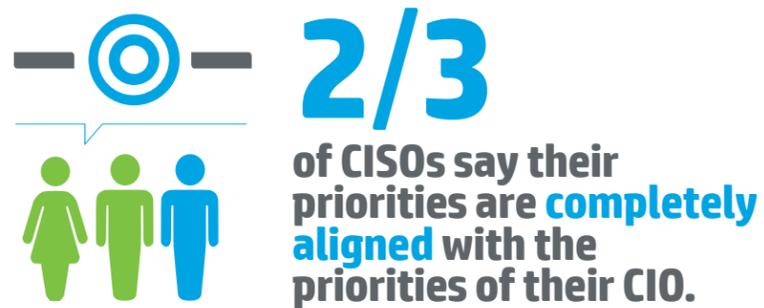


5 Steps to Secure Your Print Environment

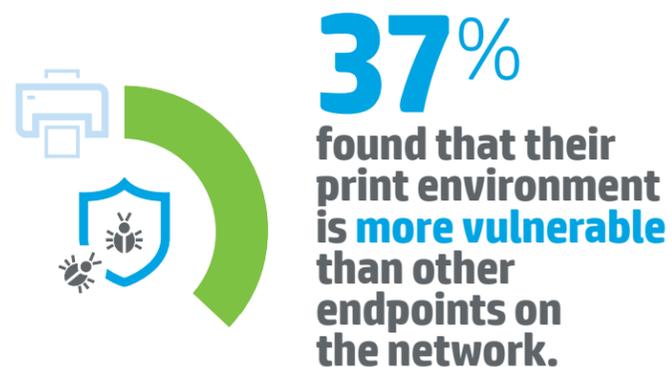
While government agencies work to combat evolving and sophisticated cyber threats to their networks, email systems and databases, they can't forget the risks associated with their print environment. In June 2016, CDG surveyed 178 government decision-makers to better understand threat levels, compliance and decision-making around print security.¹

Step 1: Align goals among key personnel

Having common security goals among decision-makers, including chief information officers (CIOs) and chief information security officers (CISOs), is an important factor in keeping data safe.

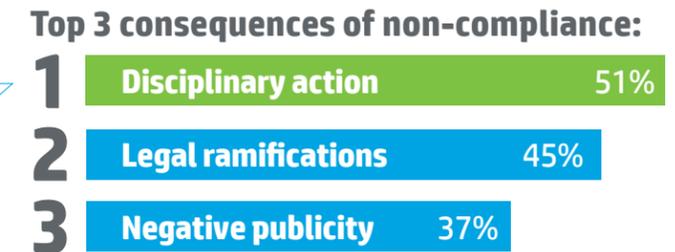


Step 2: Conduct a cybersecurity assessment



Consider potential vulnerabilities such as printer configuration, data encryption and authentication.

Step 3: Establish clear rules – and help staff follow them



Step 4: Plan for the future



Step 5: Turn to experts for help



To learn more, visit: www.hp.com/go/PrintersThatProtect

Produced by: **CENTER FOR DIGITAL GOVERNMENT**



1. The Center for Digital Government surveyed 178 state and local government IT officials in June 2016. The survey instrument was constructed in conjunction with HP, Inc. Responses were gathered from members of the *Government Technology* exchange community. All percentages noted are reflective of the survey results.