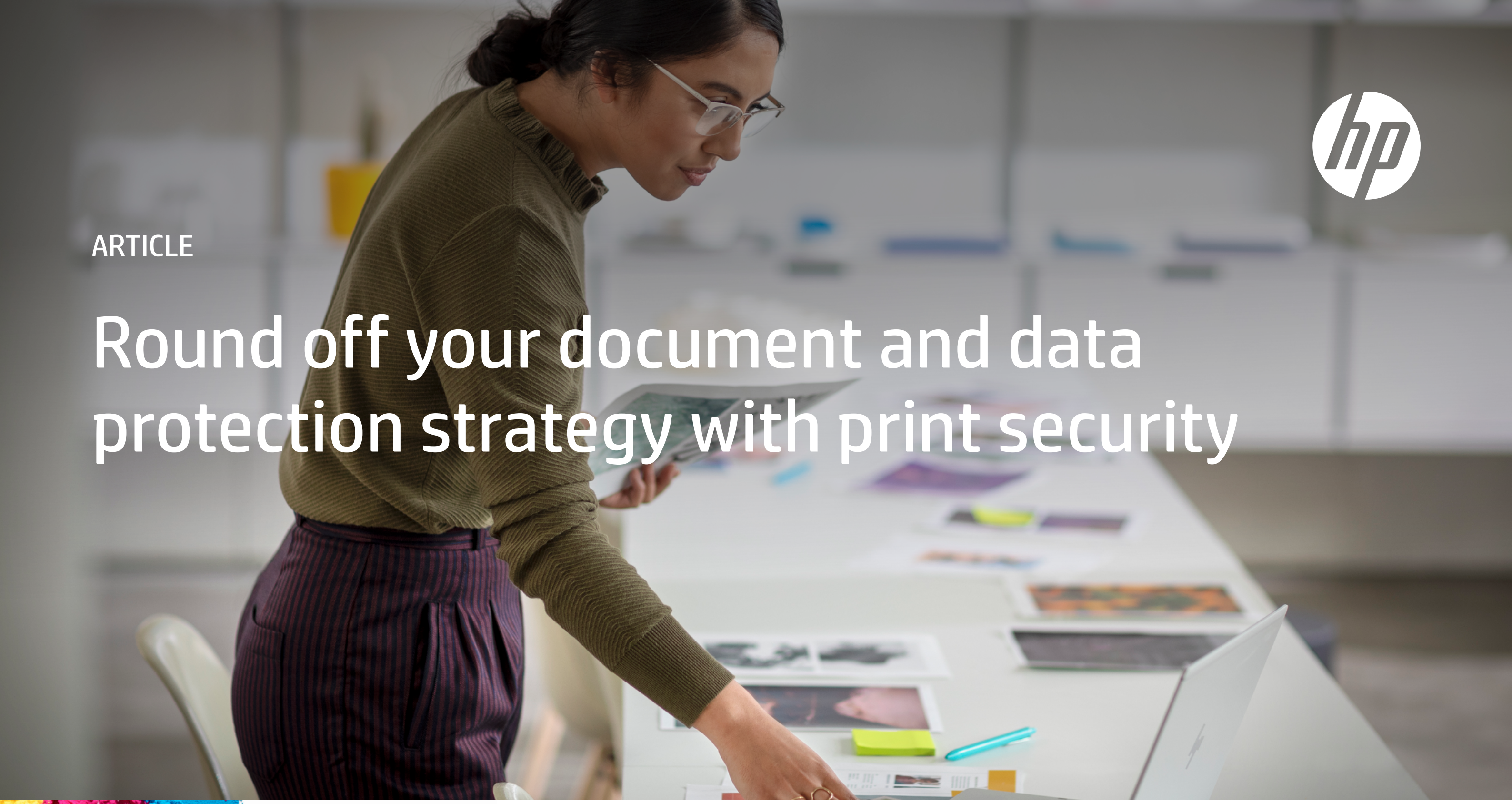
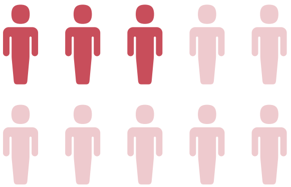


ARTICLE

Round off your document and data protection strategy with print security



Over

30%

of respondents reported one or more print-related data loss incidents.[3]

Cybercriminals are a creative bunch. From supply chain attacks to social engineering and AI-assisted attacks[1], they are endlessly devising new attack techniques and probing for blind spots in organizations' network defenses – blind spots such as the office networked printer.

As a leading enterprise technology partner, HP has been actively advocating for and enabling greater print security for organizations around the world. Even though network devices, servers, and computers are still the most targeted avenues of attack, enterprise printers are also networked endpoints. And to a cybercriminal, any unsecured endpoint is a potential attack vector.

Printers are frequently targeted

Contrary to prevailing perceptions, networked printers are targeted quite frequently by cybercriminals. According to the Global Print Security report, almost two-thirds of organizations reported a print related data loss, costing American companies a loss of over $1 million[2]. Another study cited by consulting firm Booz Allen Hamilton found that 61% of survey respondents who reported a data loss incident in 2016, at least 50% had one or more such incidents linked to a printer[3].

With Cybersecurity Ventures forecasting that cybercrime will cost the world economy $6 trillion by 2021[4], print security is no longer something that organizations can afford to ignore.

The security risks associated with printers

Before an organization can formulate a cybersecurity strategy for its networked printers, it needs to first understand the security risks that it needs to mitigate. From targeted external cyberattacks to potential malware insertion via unsecured imitation toner cartridges, sensitive documents left on a printer and more, networked printers have a variety of vulnerabilities, including[5]:

Unauthorized access to print data

Even though data security is often thought of as a digital threat, a data breach can happen from something as simple as someone walking over to the printer and accessing documents that belong to someone else.

Malware risks

Unlike Original HP Cartridges that have safeguards against tampering, many imitation cartridges use chips that can be reprogrammed to introduce malware.

Print job re-routing

With a few configuration changes, cybercriminals can redirect print jobs to their own printer.

Data manipulation

A compromised printer can allow attackers to replace or insert content into print jobs.

Data disclosure

Print data can be disclosed if an attacker has access to the printer's memory or file system, or physically from the hard drives of decommissioned printers.

Wireless printing risks

Printers with Wi-Fi printing capabilities are also vulnerable to proximity attacks, where attackers can get the printer to connect to a malicious network and execute harmful code.

Securing your printer and print data

To protect this critical endpoint, HP recommends putting basic security measures in place. To begin, select printers or managed print services from a vendor with proven security capabilities, and avoid imitation cartridges to create a strong foundation for print security. After which, round it up with timely patching of the printer's operating system, regular PIN and password changes, turning off of unused services, implementing multi-factor authentication, and providing employee training on data security best practices to strengthen your organization's security posture.

With these measures in place, you will be able to close up the hidden weakness in your security strategy and reduce the risk of a data breach originating from an under-protected networked printer.

HP's printer portfolio takes a multi-layered security approach to provide organizations with secure printing, from automatic malware detection and self-healing[6] capabilities to upgradeable firmware[7] and security tools for printer fleet management.[8] Additionally, the chips in Original HP Cartridges contain tamper-resistant firmware[9], and are designed, manufactured, and delivered with security applied throughout the supply chain to ensure product integrity.[8]

Protect your data with print solutions designed for security.
Learn more at hp.com/my/SuppliesThatProtect

REFERENCES:

[1] ZDNet, Artificial intelligence will be used to power cyberattacks, warn security experts, April 2020.

[2] Quocirca, The Print Security Landscape, 2020, Louella Fernandes, December 2020

[3] DarkReading.com, How Hackers Hit Printers, 2018.

[4] Cision, Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021, December 2018.

[5] Business News Daily, Is Your Printer Your Weak Security Link?, April 2020.

[6] HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

[7] Some printer security features enabled by future HP FutureSmart firmware upgrades may not be available on older devices, if for example, physical product characteristics limit the functionality of the new feature.

[8] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

[9] HP Office-class printing systems include Enterprise-class devices with FutureSmart firmware 4.5 or above, Pro-class devices, and their respective Original HP toner, PageWide, and ink cartridges. Does not include HP integrated printhead ink cartridges. See https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA6-8438ENW and hp.com/go/SuppliesSecurityClaims.