Round off your document and data protection strategy with print security

Data breaches are now more common and costly. A staggering

60%

of businesses reported printing data breaches of some kind.[5]

Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. At a growth rate of 15 percent, year over year – Cybersecurity Ventures also reports that cybercrime represents the greatest transfer of economic wealth in history[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 landscape report, 68% of respondents suffered print-related data losses in the past year, at an average breach cost of almost £632,000.[2]

Quocirca, surveyed 531 IT decision-makers and found that more than two-thirds of firms have experienced data loss due to printer vulnerabilities.[2]

Cybersecurity Ventures forecasted that global cybercrime will cost $10.5 trillion USD annually by 2025,[3] 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:

Unauthorized access to print data

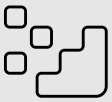
Even though data security is often thought of as a digital threat, a data breach can happen from something as simple as someone walking over to the printer and accessing documents that belong to someone else.

Malware risks

Unlike Original HP Cartridges that have safeguards against tampering,[4] 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.

“ The chips in Original HP Cartridges contain tamper-resistant firmware and are designed, manufactured, and delivered with security applied throughout the supply chain to ensure product integrity.[4]”

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 is vigilant about recognizing and mitigating security risks in the supply chain to help reduce the risk of malware entering the cartridge chip. Additionally, HP chips in Original HP office cartridges contain tamper-resistant proprietary HP firmware, which helps prevent modification by third parties after production and helps reduce the risk of malicious code entering the chip.[4]

Protect your data with print solutions designed for security.

Learn more

References:

1 Oct 2022, Embroker, 2022 Must-Know Cyber Attack Statistics and Trends

2 Nov 2021, Quocirca - Print security landscape

3 Nov 2020, Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025

4 HP office-class printing systems are select Enterprise and Managed devices with FutureSmart firmware 4.5 and up, Pro devices, LaserJet models 200 and up, with respective Original HP Toner, PageWide and Ink Cartridges. Does not include HP integrated printhead cartridges. Digital supply-chain tracking, hardware, chips and packaging security features vary locally by SKU. See www.hp.com/cartridgesecurity.

5 Jan 2022, Businesses underestimate the threat posed by vulnerable printers