IDC
Analyze the Future

IDC IN CONVERSATION

Simon Piff
Vice President, Security Practice
IDC Asia Pacific

Junaid Rehman
Security Advisor, Asia Pacific and Japan
Print Security Advisory Services
HP Inc

Print Security in the Digital Age — a Sleeping Giant Under the Hood

November 2016

Sponsored by HP Inc

As digital transformation (DX) adoption increases, organizations' exposure to potential IT risks also increases, including printer security vulnerabilities. The reality is that print security is a real and present threat as every device on the network brings with it an increase in the attack surface and potentially opens the door for any criminally minded hacker to enter.

Simon Piff, IDC's Asia Pacific head for security research, caught up with Junaid Rehman, HP Inc's Security Advisor for its print security advisory services in the Asia Pacific region and Japan, to find out more about printers as a potential sleeping giant that few organizations have taken into account where security is concerned. This IDC In Conversation interview throws the spotlight on the ongoing IT challenges such as compliance requirements, skills shortage, budget constraints, and the need for senior management buy-in to ensure nothing is left to change. Business leaders can no longer leave it to IT to "figure it out". Printer vendors like HP seek to help organizations understand where and how to fill the gaps, be it crafting an IT security policy that includes printers or educating procurement teams on the potential security risks of their printers.

Q. We have been talking about print security for a number of years now, how come this is still an issue?

A. This quote from an IT manager is typical of the perceptions in the market: "IT people are aware that printers are a security risk, but don't understand the *weight* of the risk. They think hacking into a printer just means they can print to it, not that you could steal data from it or even stage a man-in-the-middle attack on the printer."

Most companies cannot see if their printers are involved in a cyberattack because the tools used to monitor most internal endpoints are, for a wide variety of reason, not applied to printers. For example, the majority of their print devices neither have malware protection nor are they

tracking printer sys logs or connecting printer data to their SIEM systems. To compound this issue, IT managers find dealing with printers to be tedious and time-consuming.

Printers use proprietary technologies, and unlike Microsoft, Windows or Red Hat Linux, the operating system is not very open (that is why we don't have an agent from Symantec or Trend Micro for printers). You need knowledge of printers and understand all risks before mitigating risks pertaining to unsecure printers. Customers usually don't know how to approach printer security. Where to start from and which areas to cover.

All of these factors contribute to the fact that the issue still exists and companies still need to advance their print security strategies.

Q. Should printers be handled differently to other devices in the workplace?

A. Today's printers look a whole lot like PCs. They have many of the same hardware components as PCs, including disk drives, keyboards, and LCD control panels. This is true of firmware and software as well: printers have built-in operating systems, run executables, have DLLs, and run common protocols. Printers and multi-function printers (MFPs) are connected to the Internet and can be used to send emails. Today's printer is a fully functioning client on the network. From the point of view of network security, printers require the same degree of protection as PCs.

At the same time, not all printers have the same levels of criticality. The "general purpose" office printer may not need such strict controls as the printer, say, for the finance unit, but all too often, even this level of security management may not be in place.

Printers, as with all other IT systems, need to be evaluated from a risk and security perspective and then the relevant levels of control applied.

Q. What kind of threats have you seen and what was the impact?

A. Printers are a vulnerable network endpoint, like any network connected endpoint. IT managers inherently know this, but perceive that a printer hack would be fairly benign or simply malicious, such as being able to push a print-out without authorization or "take a printer down". In reality, printers can be a source to ex-filtrate company and customer data or acquire user credentials to gain further access to the network. It's quite possible for a printer to be the host of a piece of malware designed to seek out and steal user login credentials, or identify key data that has value in the open market, and become the internal launchpad for a significant data breach.

End point security risks span a variety of sources from organized crime to employee error, here are some of the vulnerability points to consider when determining how to help customers with their end point security plans.

Malware and viruses

- For endpoint devices, injection of an executable file can turn the device into a portal for hackers to steal data or hold the device for "ransom".

Device access

- Authentication management and password theft are some of the biggest IT security issues and often overlooked on printers. Less than 44% of IT managers include printers in their security strategies and less than half of these people were applying admin passwords to the printers.[1] You cannot walk into a business today and start using a laptop or desktop without first authenticating and gaining authorization to the network. However, you can find many MFPs in the hallway, or other print cubes where you can access all the features

like print, copy, scan or even email from a company account without any way to track who the email is from.

[1]*Source: Spiceworks survey of 107 IT professionals from companies with 250 or more employees in North America, Europe, the Middle East, Africa, Asia Pacific, and China, conducted on behalf of HP in January 2015.*

Data flows between devices and network and data on hard disks

- Often overlooked is the encryption of data on the printer hard disk media or use of encryption protocols for print files sent from mobile devices.
- Printing jobs can be intercepted as they travel over the network to or from a device. Risk can be a "man-in-the-middle" attack, when information is rerouted to a data capture device (like a laptop, desktop, or sniffer) before it goes to the printer. For example, college students have rerouted print jobs being sent from their professor's computer.
- It is also important to make sure that hard disks are wiped at end of life (disposal of the device) or when the device is lost or stolen.

Device configuration

- Printer configuration — most companies haven't secured their printers with admin passwords, nonetheless hardened the device settings. There are more than 250 possible security settings on an enterprise MFP. Unless you actively manage your print environment day in and day out, you cannot be confident that all of your security risks are addressed. Something as simple as a reboot can cause your entire network to be at risk.

Hardcopy document

- The shared network printer output tray is the most common place for sensitive documents —such as financial statements, proprietary data, or customer information — to fall into the wrong hands.

Fraud and counterfeit

- Deter tampering or alteration of sensitive printed documents, or theft of high-value media (i.e., prescription paper stock).

Q. Are there any best practices you can recommend for printer security?

A. Risk assessment must be done to evaluate security posture around print fleet. The Centre of Internet Security has a benchmark document for printers. There are some guidelines for securely deploying multi-function devices by the National Institute of Standards and Technology (NIST). The Australian Information Security Manual proposes that companies should take the same measures for printer security as compared to other network endpoints. Areas that we consider around print security include not only the device but also network data covering both data in transit and data at rest, access control and authentication such as who, and critically what, has access to the print infrastructure, monitoring and management, as well as the processes around this issue and, of course, document security.

Q. How does HP differentiate itself in this market?

A. HP has built its own framework for printer security. The HP Print Security Framework is built upon industry best practices, combined with government regulations and international security standards. HP takes a risk-based approach to printer security and uses its framework to conduct print security risk assessment. A risk mitigation plan and security roadmap is developed according to business requirements and security needs of organizations. HP provides comprehensive print security covering the device, data and documents.

The world of IT security has changed, and HP's goal is to continue to ensure we have the insights and installed base experience in PCs and printing to help our customers with endpoint security. We also use a holistic approach to build-in, not bolt on, security which we protect down to the BIOS in our business devices (both PCs and printers). And of course, most important are data and documents. We have advanced multi-layer authentication and encryption in-transit and at-rest with self-encrypting hard drives, and ensure our workflow solutions are compliant with regulatory requirements to address user behaviors that put confidential data on hardcopy documents at risk.

And across all of these areas, it's all about fleet-wide automation of security and we ensure customers are protected by security-based management tools. For companies without the security expertise and IT resources to manage on their own, they can always look for the right partner who have the printer security expertise, while they focus on what they do best.

ABOUT SIMON PIFF

Simon Piff runs the IT security research agenda for IDC Asia/Pacific, focusing on the needs of the chief security officer in an environment that encompasses cloud computing, the Internet of Things, and a continued and persistent attack from cybercriminals. Much has changed in this area since 1994 when he installed his first firewall, and the collision of Big Data with security, the move to a defense in-depth strategy, and the issues of insufficient numbers of well-trained staff make this a challenging area for businesses today. Having previously covered the storage system and then datacenter markets for IDC Asia/Pacific, his career background and IDC experience put him in the ideal position to deliver valuable insights to both technology buyers and providers. His background provides him with a unique understanding of the issues and challenges facing both end users and vendors with regard to their IT aspirations within the Asia/Pacific markets.

ABOUT JUNAID REHMAN

Junaid UR Rehman works as a Security Advisor in HP Inc. He provides consultancy to his managed print services teams regarding how to securely deploy and manage a printer fleet. He also helps customers in security assessments pertaining to print fleet. Junaid has over 10 years of information security experience and has helped organizations from all industries/verticals with their enterprise security strategies and implementation. He had previously worked with IBM and Oracle as security consultant and holds CISA, CISM, Mobility+, OCP 11g, ITILv3, COBIT, SABSA certificates.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com