Managed Print Services and the Role of Printers in Endpoint Security

State and local governments have become prime targets for cyberattacks. As organizations have shifted to remote work in recent months, phishing attacks have increased 85 percent and cyber breaches overall have increased 600 percent.[1]

It's more important than ever for states and localities to secure all their endpoints. Governments have traditionally focused on PCs, laptops and mobile devices connected to their networks. But printers are just as crucial to endpoint security.

As more state and local governments operate in a hybrid environment where employees split their time between home and the office, government IT teams will need to adapt to this new normal and balance efficiency and agility with enterprise security.

To achieve that balance, organizations should insist on print devices with embedded security features, and they should adopt a service-based approach to print management. Managed print services (MPS) can help governments handle the complexity of a hybrid environment and strengthen their security posture by offering a holistic, risk-based approach to endpoint security across hardware, software and firmware.

Current Challenges of Print Security

Within the public sector, the focus on print management and security tends to be an afterthought. Many state and local governments rely on legacy or custom-built systems and solutions. They may have devices in their environment that are several years old. Oftentimes, these print devices are unpatched or no longer supported.

Michael Howard, the head of HP's security and analytics practice, says it's critical for state and local governments to think about print devices as an endpoint in the same vein as a laptop, PC or mobile device.

"A printer is no different than a PC as far as how you can leverage its protocols to get on a network and then laterally move around," Howard says. "Hackers don't care where the entry point is or what type of device it is. They're usually not using that device anyway. They're using it just as a foothold in the network."

Hackers have already shown how they can exploit security vulnerabilities in printers. In one incident involving a large organization, cybercriminals hacked into a printer, accessed the organization's network, put ransomware on its data and then encrypted the data, forcing the organization to pay a ransom to regain access to the information.[2]

In one survey of IT leaders,

41% said their organizations used **network security on printers**, while

55% did so for **mobile devices** and

83% did so for **desktops and laptops**.

Recent research indicates these incidents have the potential to happen more often. In one survey of IT leaders, 41 percent of respondents said their organizations used network security on printers, while 55 percent did so for mobile devices and 83 percent did so for desktops and laptops.[3] In 2017, 11 percent of organizations reported security incidents related to printers and 59 percent reported a print-related data loss incident that year.[4] Governments could be unknowingly putting themselves at risk for similar incidents if they don't start thinking of printers as endpoints.

But changing mindsets is only half the battle. IT organizations still face other challenges as they try to secure their print assets. Limited asset management also affects their endpoint security strategy. State and local governments often lack end-to-end visibility into all the print assets within their ecosystem and therefore can't effectively manage them.

As more organizations embrace remote work, they must confront additional complexity and security vulnerabilities. Managing remote printing introduces new risks, since most employees working from home don't have printers with enterprise-grade security features and controls. Along with their colleagues, government IT teams may also begin to work remotely more frequently, which means they'll have to manage personal and office devices from the confines of their homes.

"The printer, the PC or whatever devices are in home offices — that's now the edge of the network for most organizations," Howard says. Locking down and managing those devices can be extremely difficult.

To strengthen their entire security posture, governments need to manage their print fleets holistically. They should integrate print devices that are secure and compliant by design, and they need to gain end-to-end visibility into their print assets. Adopting an MPS program can help state and local governments secure their print environment and better protect their networks.

How Managed Print Services Can Strengthen Endpoint Security

MPS encompasses several key elements:

- Services that drive innovation while helping to maximize ROI, availability and end-user satisfaction with day-to-day operational and management services.
- Secure-by-design printers that organizations can purchase or lease.
- Supplies, such as paper and other consumables required for print devices to remain operable, as well as other supplies that can actually enhance security, such as toner cartridges that can help avoid chip-based attacks with secu re smartcard technology.
- Custom print solutions that connect teams to the cloud, overcoming traditional paper-to-digital barriers to ensure data and content travel efficiently and securely across teams, tasks and workplaces.

Howard says MPS can enable state and local governments to adopt a more comprehensive approach to securing the print environment.

"A holistic approach takes it from the purchasing decision to the implementation decision to management and assessment of your print assets, in order to make sure they're safe and secure," he says.

MPS provides printer hardware and software with built-in device security features that address protection, detection and recovery. That's critically important, because printers often come with several security gaps. For one, image and print devices store sensitive information on internal devices or hard drives that can be compromised. Multifunction printers also can route jobs to other locations, which can increase the exposure of sensitive data. Unsecured cloud-based connectivity and mobile printing come with increased risks and can allow unauthorized users to gain access to sensitive information.

Additional firmware protection is another benefit of MPS. By using allow-listing capabilities to secure the underlying code

To strengthen their entire security posture, governments need to manage their printer fleet holistically. They should integrate print devices that are secure and compliant by design, and they need to gain end-to-end visibility into their print assets.

responsible for a printer fleet's core functions, firmware is automatically checked as soon as a device starts up. If the system detects an anomaly, the device automatically reboots in a secure offline mode, and the organization's IT team is notified. With this capability, state and local governments can automate their security processes and take a more proactive approach to bolstering print security without having to consume additional IT resources or a significant amount of staff time.

MPS also provides continuous monitoring of network connections to identify any anomalies or suspicious activity. In the event of an attempted malware attack, the printers' self-healing capabilities automatically trigger a reboot of systems. As governments face greater budget constraints, that kind of automation will be key to driving greater operational efficiency, better service delivery and improved enterprise security.[5]

While solutions are a critical part of MPS, so are strategic services. Security advisory services, for example, leverage experienced advisors to provide state and local governments with detailed security assessments of their print environment. Through interviews with employees and an on-site security workshop with key stakeholders, MPS providers can put together a tailored risk-mitigation plan to help an organization strengthen its endpoint security.

Another valuable service component of MPS is analytics. Predictive analytics of fleet data provides increased visibility into print assets and more proactive maintenance of these assets. That can strengthen security, increase compliance, reduce costs and minimize downtime for government agencies.

With these insights, "CSOs [chief security officers] can get actionable intelligence that tells them, 'This is where your risks are and this is how you mitigate those risks,'" Howard says.

Implementing an MPS program has already resulted in several benefits for the city of Arlington, Texas. The city, which has 3,000 employees and 900 aging printers and copiers, decided to implement an MPS program to improve its efficiency, lower costs and enhance security.

After launching its program, Arlington upgraded most of its assets to next-generation printers to facilitate high-volume printing and remote management, improve its workflows and to secure its print environment. The move has given the city access to solutions with embedded security features such as allow-listing, encryption, authentication and advanced firmware protection. The city has gained more visibility into its print environment while benefiting from enhanced security. Arlington also has increased employee productivity and reduced costs across 16 departments.[6]

Moving away from a fragmented approach to print security and launching an MPS program could produce similar gains in efficiency, productivity and security for other government organizations.

Conclusion

MPS can enable state and local governments to formulate and execute a more robust print security strategy.

Governments need to begin looking at print devices as endpoints in the same way they view laptops, desktops and mobile devices. A trusted MPS provider can help an organization shift its approach and identify strategies and solutions that will enhance print security.

Before enlisting the help of an MPS provider, governments should first determine their key security requirements and then assess potential strategic partners based on whether they offer a holistic, risk-based approach to match these business needs. A provider should speak to an organization "not just in print language but also security language," Howard says.

Experienced MPS providers have core competencies in print and document workflow, content management and secure print services, and they offer remote monitoring and management capabilities. Additionally, the right provider should offer security advisory, analytics and remote work services that ensure the print environment is secure at every level — both inside and outside the office.

Securing printers isn't a one-time event. It's an ongoing process that requires strong asset management: An organization needs to know where all of its devices are located, who is using them and how they're being used. MPS can empower state and local governments with all the capabilities they need to ensure that printers are no longer vulnerable endpoints for hackers to exploit.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from HP.

Endnotes:
1. Michael Howard SME Interview
2. https://www.govloop.com/printer-security-afterthought/
3. https://h41369.www4.hp.com/taw/article/PR/GB/TAW_001952
4. http://h20195.www2.hp.com/v2/getpdf.aspx/4AA6-9168ENW.pdf
5. http://h20195.www2.hp.com/v2/getpdf.aspx/4AA6-9168ENW.pdf
6. https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-3788ENW

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**.

For: hp

HP Inc. creates technology that makes life better for everyone, everywhere — every person, every organization, and every community around the globe.