Why every business needs a smart printing services strategy

All businesses need a strategy for printing services for security and productivity. HP Print Security Advisors Jason O'Keefe and Michael Howard explain why.

Learn more

"Most companies don't think they need security for their print infrastructures, so print is very low on their priority list for security"

Jason O'Keefe, HP Print Security Advisor

Network-connected printers are more insecure than most organisations realise. With security threats on the rise—and getting absolutely disastrous—businesses of all sizes need printing services strategies to protect their organisations and minimize risk. At the core of crafting a strong strategy for many businesses is working with a managed print service provider that can identify and plug security vulnerabilities, as well as take care of issues (think: equipment maintenance), so printing never gets in the way of productivity.

Addressing printer insecurity

According to a survey of over 2,000 global IT security practitioners—conducted by the Ponemon Institute—60 percent of respondents acknowledge that a data breach involving a network-connected printer has likely occurred, and most respondents predict a data breach resulting from insecure network-connected printers in the next 12 months.

But only 34 percent of respondents said their organisation has a process for restricting access to high-risk printers, including printed, hard-copy documents. These glaring security gaps can leave small and midsize businesses in particular open to attacks that are expensive at best and crippling at worst.

Jason O'Keefe, HP Print Security Advisor, said most organisations underestimate how vulnerable they are through their print infrastructures.

"Most companies don't think they need security for their print infrastructures, so print is very low on their priority list for security," he said. "We present our framework, which has up to 200 controls that we evaluate for vulnerabilities across the print infrastructure. All of a sudden, eyes widen, and the tune changes completely. The initial scepticism becomes disbelief and shock, which then opens the floor for a very frank and lively discussion."

A good printing services strategy should start with an evaluation of vulnerabilities. According to Michael Howard, HP Chief Security Advisor, most print-based security vulnerabilities boil down to four factors: aging technology; failure to implement security controls properly; heterogeneous vendor environments; and unmanaged print environments.

Did you know the average organisation has around six users per printer? While computers and laptops may get locked down between uses, printers don't follow the same protocols—leaving a vulnerability for every six users. "Many security teams could not tell you how many print devices exist in their environments. There could be 5,000 devices—all open," said Howard. "When you think about how pervasive print is in most organisations, the lack of proactive security is shocking and scary."

Why printing services strategies matter

A smart printing strategy locks down printers (just like with computers), limits administrative privileges, implements username and password guidelines, and provides monitoring. This is key to creating visibility, traceability, and accountability.

"Visibility is essential," O'Keefe said. "I would also highlight collaboration as key to effective print security. To gain the rich intelligence required for robust security, companies have to break down the barriers between print administrators, security pros, and internal audit staff. These groups have to be willing to work together to secure a key part of the network that has been overlooked for years."

In addition, organisations can remediate their print-based vulnerabilities by:

- Consistently updating firmware
- Reducing administration across the print infrastructure
- Upgrading print databases from express to enterprise editions
- Implementing processes and documentation to keep security consistent and measurable
- Providing security awareness training to print administrators.

"Print security, just like corporate security, is an ongoing process," Howard said. "As a result, it's critical to pursue constant improvement through deeper assessment and expert advice."

Deeper, ongoing assessment is connected with the importance of governance. For print, governance should include user account management (who's accessing the print infrastructure), compliance to corporate policies, risk management, security documentation, and event logging.

"Print security, just like corporate security, is an ongoing process,"

Michael Howard, HP Chief Security Advisor

Managed or unmanaged – that is the question

A solid strategy requires a wide range of components. For most businesses, particularly small and midsize businesses, crafting and executing this type of strategy in house just isn't in the cards. They'd rather dedicate their time and energy to actually running the business. Working with managed printing services providers, who can handle all the nitty-gritty details and deliver the level of security that businesses need to run smoothly, is a quality solution.

Step one to creating a smart printing strategy is to ask questions. To start, what printers are right for our organisation? Should we go with ink or laser printers? What printing features do we need? Answering these questions requires balancing reliability, cost, and performance.

Next, businesses should think about security, maintenance, and support. Should we handle our printers in house or work with a provider? Under this question, there are others, like: Is our IT team equipped to deal with printer problems? Will it cost more to handle print services in house over the long run? For smaller businesses, the answer is often yes.

Businesses that choose a managed printing service should think about when to consider a contract, as well as which provider to work with. This requires asking questions like: What are the services we need? What goes into the service-level agreement? How much will this cost? How quickly are we expecting to grow our printer network? As we grow, how does the printing strategy need to change?

The dangers of unsecured network connected printers are clear, and businesses of all sizes need to make printing services part of their overall approach to security and productivity. Fortunately, there are solutions providers out there to handle the dirty work.

Learn more
hp.com

4AA7-1720EEE, November 2017