STRENGTHENING OVERLOOKED POINTS OF DATA SECURITY

Better print management can help government improve data protection and work efficiency.

Printers are a fundamental tool for all types of government work and citizen service. But printers can also be a significant point of vulnerability for information security.

By taking a fresh look at print management, government IT departments can help improve data protection, security practices, and workflows across their organizations.

Weak Confidence in Current Security

Government IT staff and leaders should have a high level of confidence about the security measures in place for all systems, applications, and devices. Yet, According to a survey conducted by Quocirca in 2019, print is considered to be one of the top security risks to any organization. In fact, 66% rank print in their top 5 risks.[1]

Poor information security can lead to costly consequences. The cost of a data breach is estimated at over $8.19 M,[2] which may include legal fees, regulatory fines, credit monitoring, IT repair, and other services.

Implementing redundant data protection by adding security layers for multiple touchpoints and functions in a workflow—including for printers—is critical for all organizations, especially those in government.

Why Strengthen Information Security?

Government agencies store many types of personal information that appeal to hackers. Information about employees, program clients, vendors, and citizens may include Social Security and driver's license numbers, financial and tax information, or health records. In 2019 the average data breach had 32,434 records.[2] The effects of a breach can be severe, leading to long-term impacts on employee productivity and erosion of public trust.

At the same time, data privacy regulations are becoming more stringent. Government agencies may already be required to comply with federal regulations for data security, such as the Health Insurance Portability and Accountability Act (HIPAA) and industry standards like the Payment Card Industry Data Security Standard (PCI-DSS). States are also taking a more active role in regulating cybersecurity. At least 19 states have laws that specify data protections for state agencies.[3] In 2017, more than 240 bills related to cybersecurity across the public and private sectors were introduced in state legislatures.[4]

Recognizing Potential Security Vulnerabilities in Printers

State and local governments might consider printers a lower priority than other information security investments. However, according to the Quocirca survey, 87% of the respondents state that print will still play an important role in business processes, even in two years' time.[5]

However, several factors present a compelling case for strengthening security around printers and workflows. The first is that printers and printed documents can be a weak link in an organization's security strategy. According to a security consulting firm, 13 percent of the incidents it handled in 2016 involved compromised paper records.[2]

Network-connected printers—especially those that were not designed or configured with external security in mind—can create several types of vulnerabilities. A single printer with a weak administrative password or an open port configuration could be used by hackers to access a government's network for data theft, installation of ransomware and malware, or application attack. Hackers may also potentially intercept sensitive documents sent to a printer. Confidential personal information, stored in files on the printer's hard drive, may be easy to view and copy—especially if the hard drive is not encrypted or wiped prior to printer disposal.

In addition, government is going mobile, and field workers and other employees expect to be able to send documents from a laptop, tablet, or smartphone to a printer over a wireless connection. However, a mobile printing service can increase vulnerability unless it is adequately secured and offers an efficient, simple workflow.

Finally, government leaders should be aware of security threats at the device. Something as simple as leaving documents in an output tray can expose sensitive information. Controls are also essential for scanning documents, receiving faxes, or transferring documents to the cloud to reduce the risk of information exposure and theft.

Improving Information Security with Print Management

A print management solution can give IT more control over how information is acquired via printers and then distributed across the internal network, to private cloud storage or applications, or to a public internet site. This control helps protect sensitive information by providing an audit trail for information access and distribution across departments, locations, and programs.

WHAT'S IN A PRINT MANAGEMENT SOLUTION?

A print management solution coordinates all the print, scan, fax, and share processes in an agency.

Access Control	Document Security	Data Protection	Network Security
Authenticate a user prior to printing.	Protect sensitive documents with printer encryption and a secure repository.	Erase images when job is complete.	Implement routine vulnerability assessments to help identify gaps in your security posture.
Control user access at the file level via enterprise digital rights management (EDRM) tools.	Prevent unattended printing.	Protect printer passwords and encryption keys with separate, tamper-resistant element.	Intercept and prevent scans and prints from being sent using control words.
	Create an audit trail of user actions with documents.	Wipe data from hard drive when printer is removed from service.	Route incoming faxes to a password-protected network folder before printing.

Print management tools can also help governments meet regulatory compliance obligations by helping to prevent unauthorized access to sensitive data on printed documents. Features such as authentication require users to verify their identity with a password or access card before printing a document. Predefined user credentials can also be used to restrict access to certain printer functions and document types based on a person's role.

These capabilities are designed to offer critical, transparent layers of protection that enhance other IT and network security measures already in place. They may also help maintain public trust, especially when it comes to the privacy of citizen and employee data.

Streamlining Workflows and Productivity

A print management solution can also streamline workflows to improve productivity, transparency, and cost control. For example, many government activities require the ability to capture, move, and collaborate on information in multiple workflows. A print management solution offers these capabilities while also helping to control access to those documents at input, distribution, and output points. In addition, indexing and metadata features make documents easy to search and classify, which can save time and costs involved in managing public records.

With the right print management strategy, agencies can increase efficiency by reducing repetitive tasks, improve transparency by making the right information accessible to those who need it, and enhance cost control by developing consistent, secure processes for information sharing.

Managing the Transition to Print Management

The growing number of regulatory requirements means everyone needs to help with compliance. Yet, employees may not know the risks involved with printers or how printing may impact their regulatory compliance.

Best Practices for Securing Data with Print Management

- Apply management principles and processes consistently across all printers in the agency.
- Consider how user, device, and application workflows can be modified to help improve security and efficiency.
- Identify the specific information types that need protection (including personal data) and regulatory requirements for data access and distribution.
- Plan a transition process that helps users understand the ease and value of adopting new security technologies and practices.
- Look at how print management can improve the availability of printing services across departments and locations.

If an agency adopts an information security policy without streamlining technology and processes, users will not necessarily embrace the change. Implementing easy-to-understand, seamless, and reliable print management technology can encourage users to safeguard confidential, restricted, and sensitive information, especially personal data.

Print management with intuitive security features can encourage employees to accept new printing processes and printer access requirements. When information security is integrated with printing, it becomes transparent and helps users comply with the agency's information security policies and regulatory requirements.

Targeted and regularly updated training is also important to maintain security awareness and practices. Although, According to the Quocirca survey, organizations vary in their capability to ensure the security of their print environment. Only 27% of the respondents were classified as print security leaders.[5]

A Strategy for Better Security and Better Work

Security vulnerabilities will only continue to grow. By taking a proactive and strategic approach to print management, governments can create vital redundancies in security measures. In doing so, they will also improve workflows for more efficient processes and service delivery.

Endnotes

1. *2019 Quocirca - Global print security landscape.*
2. *2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.*
3. *https://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReportSummary2017.pdf.*
4. *http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx.*
5. *2019 Quocirca - Global print security landscape*

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

PRODUCED BY

CENTER FOR DIGITAL EDUCATION

SPONSORED BY

Canon

CANON SOLUTIONS AMERICA

01/19-920-3982